

## 明細書

### 情報処理システム及び情報処理装置

#### 技術分野

本発明は、情報処理システム及び情報処理装置に関し、例えば生体固有の血管に基づくデータを認証する場合に適用して好適なものである。

#### 背景技術

従来、生体固有となる血管の形成パターン（以下、これを血管形成パターンと呼ぶ）に基づいて認証処理を実行する認証装置が提案されている。

この種の認証装置においては、血管に内在する脱酸素化ヘモグロビン（静脈血）又は酸素化ヘモグロビン（動脈血）に近赤外線帯域の光が特異的に吸収されることを利用して登録者の血管を撮像し、この撮像結果として得られる血管画像から血管形成パターン（以下、これを登録血管形成パターンと呼ぶ）を抽出し、これを所定のデータベースに登録しておく。

そして認証装置は、この登録処理と同様にして認証対象者における血管形成パターン（以下、これを認証対象者血管形成パターンと呼ぶ）を抽出し、この認証対象者血管形成パターンを、予めデータベースに登録しておいた複数の登録血管形成パターンと順次照合するようにして、本人（登録者）の有無を判定するようになされている（例えば特許文献1参照）。

特許文献1 特願2003-242492公報。

しかしながらこのような認証装置においては、認証対象者血管形成パターンに対応する登録血管形成パターンが検出されるまで、複数の登録血管形成パターンを順次照合するため、認証対象者血管形成パターンと照合す

る処理時間が増大する傾向にあり、ユーザにとっては待ち時間が長くなるという問題があった。

殊に、データベースに登録される登録血管形成パターンが多くなるほど、かかる処理時間は増大する傾向にあることから、ユーザの待ち時間はより長くなるといった結果を招くことになる。

### 発明の開示

本発明は以上の点を考慮してなされたもので、使い勝手を格段的に向上させ得る情報処理システム及び情報処理装置を提案するものである。

かかる課題を解決するために本発明は、第1の情報処理装置と、第2の情報処理装置とによって構成される情報処理システムであって、第1の情報処理装置には、生体の所定部位における識別対象を生体識別データとして記憶する記憶手段と、生体に保持されて所定の位置にまで近接され、当該位置に近接された状態で通信する第1の通信手段とを設け、第2の情報処理装置には、位置に近接された生体を生体データとして検出する生体センサと、位置に近接された生体に保持される第1の通信手段と通信する第2の通信手段と、生体センサで検出された生体データから所定部位に対応する生体データを抽出する抽出手段と、抽出手段で抽出された所定部位に対応する生体データと、第1及び第2の通信手段を介して第1の情報処理装置から取得した生体識別データに基づいて生体認証する生体認証手段とを設けるようにした。

従ってこの情報処理システムでは、第1の情報処理装置を第2の情報処理装置に近接させるだけで、当該第2の情報処理装置が、このときこの第1の情報処理装置を保持するユーザの生体データを自動的に取得できるため、複数の第1の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして第2の情報処理装置に登録する場合に比して、当該第2の情報処理装置におけるデータベースから各生体識別データを任意

の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間大幅に短縮することができる。

また本発明は、情報処理装置であって、所定の位置に近接された生体を生体データとして検出する生体センサと、その位置に近接された生体に保持される通信対象と通信する近距離通信手段と、生体センサで検出された生体データから所定部位における生体データを抽出する抽出手段と、抽出手段で抽出された所定部位における生体データと、通信対象に登録され、当該通信対象から近距離通信手段を介して取得した生体識別データとに基づいて照合する生体認証手段とを設けるようにした。

従ってこの情報処理装置では、通信対象が近接されるだけで、その通信対象を保持するユーザの生体データを自動的に取得できるため、複数の通信対象にそれぞれ記憶される全ての生体識別データをデータベースとして登録しておけば場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間を大幅に短縮することができる。

さらに本発明は、情報処理装置であって、生体の所定部位に装着する装着手段と、所定部位における識別対象を生体識別データとして記憶する記憶手段と、装着手段に保持され、当該装着手段を装着した所定部位を近接させた通信対象に対して生体識別データを送信する通信手段とを設げ、当該装着手段を装着した状態で近接された生体が通信対象において生体データとして検出されるようにした。

従ってこの情報処理装置では、所定部位に装着した装着手段が通信対象に近接させるだけで、その通信対象を保持するユーザの生体データが自動的に取得されるため、複数の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして通信対象に登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間を大

幅に短縮するさとができる。

本発明の情報処理システムによれば、第1の情報処理装置を第2の情報処理装置に近接させるだけで、当該第2の情報処理装置が、このヒキこの第1の情報処理装置を保持するユーザの生体データを自動的に取扱できるようにしたことにより、複数の第1の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして第2の情報処理装置に登録する場合に比して、当該第2の情報処理装置におけるデータベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間の短縮に応じてユーザの待ち時間を短縮化することができ、かくして使い勝手を格段的に向上させることができ。

また本発明の情報処理装置によれば、通信対象が近接されるだけで、その通信対象を保持するユーザの生体データを自動的に取得できる上うにしたことにより、複数の通信対象にそれぞれ記憶される全ての生体識別データをデータベースとして登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間の短縮に応じてユーザの待ち時間を短縮化することができ、かくして、使い勝手を格段的に向上させることができ。

さらに本発明の情報処理装置によれば、所定部位に装着した装着手段を通信対象に近接させるだけで、その通信対象を保持するユーザの生体データが自動的に取得されるようにしたことにより、複数の情報処理装置にそれぞれ記憶される全ての生体識別データをデータベースとして通信対象に登録しておく場合に比して、当該データベースから各生体識別データを任意の順序で読み出して照合するといった処理を回避することができ、その処理に費やされる時間の短縮に応じてユーザの待ち時間を短縮化することができ、かくして使い勝手を格段的に向上させることができ。

## 図面の簡単な説明

図1は、第1の実施の形態による情報処理システムの全体構成を示す略線図である。

図2は、カード端末と認証装置との構成(1)を示す略線図である。

図3は、カード端末と認証装置との構成(2)を示す略線図である。

図4は、近赤外光の光路(1)を示す略線図である。

図5は、第1の実施の形態による端末側信号処理部と認証側認証処理部との具体的な回路構成を示す略線図である。

図6は、第1の認証処理手順を示すフローチャートである。

図7は、第2の実施の形態による情報処理システムの全体構成を示す略線図である。

図8は、リング端末の構成を示す略線図である。

図9は、リング端末と認証装置との構成(1)を示す略線図である。

図10は、リング端末と認証装置との構成(2)を示す略線図である。

図11は、第2の実施の形態による端末側信号処理部と認証側認証処理部との具体的な回路構成を示す略線図である。

図12は、近赤外光の光路(2)を示す略線図である。

図13は、第2の認証処理手順を示すフローチャートである。

図14は、他の実施の形態による生体認証(1)を示す略線図である。

図15は、第3の認証処理手順を示すフローチャートである。

図16は、他の実施の形態による生体認証(2)を示す略線図である。

図17は、第4の認証処理手順を示すフローチャートである。

図18は、他の実施の形態による生体認証(3)を示す略線図である。

図19は、第5の認証処理手順を示すフローチャートである。

図20は、データ送信処理と生体認証処理との関係を示す略線図である

。

## 発明を実施するための最良の形態

以下図面について、本発明の一実施の形態を詳述する。

### (1) 第1の実施の形態

#### (1-1) 第1の実施の形態による情報処理システムの全体構成

図1において、1は全体として第1の実施の形態による情報処理システムを示し、カード形状でなる複数の端末装置（以下、これをカード端末と呼ぶ） $2_i$  ( $i = 1, 2, \dots, N$ ) と、認証装置3と、カード端末管理サーバ4とによって構成される。

各カード端末 $2_i$ は、所定のサービスの提供対象となるユーザにそれぞれ発行されたものであり、当該ユーザに内在する血管の形成パターン（以下、これを血管形成パターンと呼ぶ）を登録データ（以下、これを登録血管パターンデータと呼ぶ）としてそれぞれ保持している。

一方、認証装置3は、所定の設置箇所に設置されており、サービスを受けようとするユーザが血管形成パターンを登録した正規ユーザ（以下、これを登録者と呼ぶ）本人であるか否かを、各カード端末 $2_i$ にそれぞれ保持されている登録血管パターンデータに基づいて判定するようになされている。なお、この情報処理システム1では、1つの認証装置3を設置する場合であるが、複数の認証装置3を所定の設置箇所に設置するようにしても良い。

他方、カード端末管理サーバ4は、各カード端末 $2_i$ を、当該カード端末 $2_i$ にそれぞれ保持された固有の端末ID（Identifier）に基づいて管理するようになされている。

この情報処理システム1では、サービスを提供する場合、ユーザはカード端末 $2_x$  ( $x = 1, 2, \dots, N$ ) を認証装置3の所定位置にかざすように近接する。この場合、認証装置3は、カード端末 $2_x$ を近接させたユーザの手における血管形成パターンを取得すると共に、端末IDに基

づくカード端末 $2_x$ と、カード端末管理サーバ $4$ との相互認証を中継する。また認証装置 $3$ は、この相互認証結果に応じてカード端末 $2_x$ に保持された登録血管パターンデータを取得する。

この状態において認証装置 $3$ は、ユーザから取得した血管形成パターンと、カード端末 $2_x$ から取得した登録血管パターンデータに表される血管形成パターンとを照合することによって登録者本人の有無を判定するようになされている。

このようにこの情報処理システム $1$ では、カード端末 $2_x$ を認証装置 $3$ に近接させるだけで、当該認証装置 $3$ が、このときこのカード端末 $2_x$ を把持するユーザの血管形成パターンを自動的に取得し、この血管形成パターンと、当該カード端末 $2_x$ に予め登録された血管形成パターンとを照合する。

従ってこの情報処理システム $1$ では、複数のカード端末 $2_i$ にそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置 $3$ に登録する場合に比して、当該認証装置 $3$ におけるデータベースから各血管形成パターンを任意の順序で読み出して照合するといった処理を回避することができるため、その処理に費やされる時間を大幅に短縮することができるようになされている。

またこの情報処理システム $1$ では、複数のカード端末 $2_i$ にそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置 $3$ に登録する場合に比して、当該データベースに登録された血管形成パターンが認証装置 $3$ の管理者等によって盗用されるといったことを回避することができるため、当該血管形成パターンの信頼性を向上することができるようになされている。

さらにこの情報処理システム $1$ においては、生体の内方に介在する固有構造物の血管を認証対象として選定することによって、生体表面に有する指紋等を認証対象とする場合に比して、生体からの直接的な盗用のみなら

ず第三者による登録者への成りすましをも防止できるようになされている。  
。

#### (1-2) カード端末及び認証装置の構成

ここで、カード端末2x及び認証装置3の構成を図2及び図3に示す。

このカード端末2xには、アンテナコイル（以下、これを端末側アンテナと呼ぶ）AT<sub>CD</sub>と、当該端末側アンテナAT<sub>CD</sub>に接続された信号処理部（以下、これを端末側信号処理部と呼ぶ）IC<sub>CD</sub>1とが所定位置に内蔵されており、当該端末側信号処理部IC<sub>CD</sub>1には、端末ID及び登録血管バターンデータが登録されている。

この端末側信号処理部IC<sub>CD</sub>1は、認証装置3から供給される電磁誘導信号を端末側アンテナAT<sub>CD</sub>を介して受信した場合、その受信に応じて誘起される電圧を駆動電圧として起動し、認証装置3及びネットワークNT（図1）を介してカード端末管理サーバ4との間で各種データ授受することによって相互認証する。

また端末側信号処理部IC<sub>CD</sub>1は、この相互認証結果に応じて認証装置3から供給され暗号データを用いて登録血管バターンデータを暗号化し、当該暗号化した登録血管バターンデータを端末側アンテナAT<sub>CD</sub>を介して認証装置3に送信するようになされている。

一方、この認証装置3は、例えば角筒状であり、当該認証装置3の筐体には、カード端末2xを近接させる面（以下、これを近接面と呼ぶ）3Aが選定されている。この近接面3Aには、無色透明のガラス材質である開口窓OWが形成され、当該開口窓OWを囲むようにアンテナコイル（以下、これを認証側アンテナと呼ぶ）AT<sub>o</sub>が設けられている。

この認証側アンテナAT<sub>o</sub>は、認証装置3の筐体内の所定位置に内蔵された信号処理部（以下、これを認証側信号処理部と呼ぶ）IC<sub>o</sub>,1に接続される。認証側信号処理部IC<sub>o</sub>,1は、認証側アンテナAT<sub>o</sub>を介して電磁誘導信号を発信するようになされており、当該電磁誘導信号によ

って、近接面3Aに近接されたカード端末2Xをパッシバレス状態で起動させ得るようになされている。

かかる構成に加えてこの認証側信号処理部IC<sub>o,r</sub>1には、近接面3Aに近接させたカード端末2Xを持する手の内方における血管を読み取る生体情報読取部LIRが接続されている。この生体情報読取部LIRは、開口窓OWの下方に設けられた撮像カメラCM(図3)と、近接面3Aの所定位置に設げられた1又は2以上の近赤外光光源LSとからなっている。

この実施の形態の場合、カード端末2Xを持する手と、近接面3Aとは所定の位置関係を保って近接するようになされており、例えば、図3に示したように、当該手の指における指腹を、近接面3Aに対して平行となる状態かつ所定方向DRから対向させた状態で近接するようになされている。

なお、この近接面3Aに対して手を能動的に近接するようにしても良く、あるいは、所定の位置に配置させるための部材(図示せず)を介して受動的に近接するようにしても良い。また端末側信号処理部IC<sub>CD</sub>1(図2)に予め記憶されている登録血管パターンデータは、近接面3Aに対して所定の位置関係にある手から抽出された血管形成パターンを表すデータとなっている。

このようにしてカード端末2Xを持した手を近接面3Aに近接させた場合、認証側信号処理部IC<sub>o,r</sub>1には、カード端末2Xの起動に応じてそのカード端末2Xから、相互認証に関するデータが供給される。

この場合、認証側信号処理部IC<sub>o,r</sub>1は、ネットワークNT(図1)を介してカード端末管理サーバ4(図1)に接続し、相互認証に関するネットワークNTを介してカード端末管理サーバ4に送信する。また認証側信号処理部IC<sub>o,r</sub>1は、カード端末管理サーバ4から供給される相互認証に関するデータを受信すると、当該データを認証側アンテナAT<sub>o,r</sub>を

介してカード端末2xに送信する。

その一方で、認証側信号処理部IC。,1は、生体情報読取部LIRを駆動する。この場合、図4において破線で示すように、近赤外光光源LSから撮像空間に発射される近赤外光は、カード端末2xを把持する手の指に照射され、当該指に内在する血管を通るヘモグロビンに吸収されると共に血管以外の組織で散乱及び反射してその指から出射する。この出射した近赤外光は、血管を投影する近赤外光（以下、これを血管投影光と呼ぶ）として得られ、この血管投影光が、開口窓OW（図1）から撮像カメラCMの撮像レンズ10a、絞り（図示せず）及び近赤外光透過フィルタ10bを順次介して固体撮像素子10cに入射することとなる。

認証側信号処理部IC。,1は、撮像カメラCMを制御して撮像レンズ10aの焦点距離及びフォーカス位置を調整すると共に、固体撮像素子10cに入射する血管投影光の光量を調整する。そして認証側信号処理部IC。,1は、固体撮像素子10cの撮像面に結像される血管を所定周期で血管画像信号として生成し、当該血管画像信号から血管形成パターンを抽出する。

また認証側信号処理部IC。,1は、カード端末2xと、カード端末管理サーバ4との相互認証の成功した場合、当該成功に応じて所定の暗号鍵を認証側アンテナAT。,を介してカード端末2xに送信する。そして認証側信号処理部IC。,1は、カード端末2xから、この暗号鍵Zにより暗号化された登録血管パターンデータを認証側アンテナAT。,を介して受信すると、これを復号化する。

このようにして認証側信号処理部IC。,1は、撮像対象のユーザから抽出した血管形成パターンと、カード端末2xに登録された登録血管パターンデータに表される血管形成パターンとを取得する。

そして認証側信号処理部IC。,1は、これら血管形成パターンを照合し、当該照合結果に応じて登録者本人の有無を判定するようになされている。

る。ちなみにこの判定結果は、この認証装置内に搭載されたサービス提供処理部又はこの認証装置3外に接続されたサービス提供処理部に通知され、当該サービス提供処理部によって所定のサービスが登録者に提供されることと低る。

#### (1-3) 信号処理部の具体的な回路構成

次に、上述した端末側信号処理部IC<sub>CD</sub>1及び認証側信号処理部IC<sub>C</sub>,1の具体的な回路構成について説明する。

図5において、カード端末2xの端末側信号処理部IC<sub>CD</sub>1、この端末側信号処理部IC<sub>CD</sub>1全体の制御を司るCPU((Central Processing Unit)以下、端末側CPUと呼ぶ)21に対して、プログラムや各種設定データ等が記憶されたROM(Read Only Memory)、ワークメモリとしてのRAM(Random Access Memory)及び各種パラメータが格納されたEEPROM(Electrically Erasable Programmable Read only Memory)からなる内部メモリ22と、電磁誘導方式に準拠して各種信号を送受信する送受信部23と、暗号化/復号化部24と、乱数発生部25とをそれぞれバス26を介して相互に接続して構成される。

この送受信部23は、認証装置3から供給される電磁誘導信号を端末側アンテナAT<sub>CD</sub>を介して受けると、これに応じて誘起される電圧を内蔵バッテリ(図示せず)蓄積するようになされている。この蓄積した電圧は、所定の閾値まで達すると、駆動電圧として各回路部に供給され、この結果、カード端末2xが起動することとなる。

この状態において端末側CPU21は、内部メモリ22のROMに格納されたプログラム及び設定データに基づいて、起動した旨を通知する起動通知データD1を生成する。そして端末側CPU21は、この起動通知データD1を送受信部23及び端末側アンテナAT<sub>CD</sub>を順次介して認証装

置 3 に送信すると共に、各回路部を制御してカード端末管理サーバ 4 と相互認証するようになされている。

一方、認証装置 3 の認証側信号処理部 C P U 3 1 は、この認証側信号処理部 C P U 3 1 全体の制御を司る C P U (以下、これを認証側 C P U と呼ぶ) 3 1 に対して、プログラムや各種設定データ等が記憶された R O M s 当該認証側 C P U 3 1 のワークメモリとしての R A M 及び各種パラメータが格納された E E P R O M からなる内部メモリ 3 2 と、電磁誘導方式に準拠して各種信号を送受信する送受信部 3 3 と、暗号化ノ復号化部 3 4 と、ネットワークインターフェース 3 5 と、生体情報読取部 L I R を駆動制御する駆動制御部 3 6 と、生体情報読取部 L I R での読み取り結果から血管形成パターンを抽出するパターン抽出部 3 7 と、認証部 3 8 とをそれぞれバス 3 9 を介して相互に接続して構成される。

この送受信部 3 3 は、電磁誘導信号を認証側アンテナ A T 3 0 を介して発信するようになされており、当該電磁誘導信号によって起動したカード端末 2 x から送信される起動通知データ D 1 を認証側アンテナ A T 3 0 を介して受信すると、これを認証側 C P U 3 1 に送出する。

認証側 C P U 3 1 は、送受信部 3 3 から供給される起動通知データ D 1 を受けると、内部メモリ 3 2 の R O M に格納されたプログラム及び設定データに基づいて各回路部を制御し、カード端末 2 x と、カード端末管理サーバ 4 との相互認証を中継するようになされている。

#### (1-4) 相互認証の申継処理

ここで、かかる認証装置 3 における相互認証の中継処理を、カード端末 2 x と認証装置 3 とにおける相互認証とともに詳細に説明する。

実際上、端末側 C P U 2 1 は、起動に応じて、端末 I D をシード ( S e e d ) とするデータ (以下、これをシードデータと呼ぶ) D 2 a と、当該シードデータ D 2 a を拡散するデータ (以下、これを拡散データと呼ぶ) D 2 b とを生成し、これらを乱数発生部 2 5 に送出する。

乱数発生部 25は、シードデータD2aを拡散データD2bにより拡散することによって乱数パターンのデータ（以下、これを乱数パターンデータと呼ぶ）D3を生成し、これを暗号化ノ復号化部24に送出する。

暗号化ノ復号化部24は、この乱数パターンデータD3に対して、予め保持している鍵情報を用いて例えばDES(Data Encryption Standard)等の所定の暗号化処理を施し、この結果得られる暗号化乱数パーシデータD4を送受信部23及び端末側アンテナAT<sub>CD</sub>を順次介して認証装置3に送信する。

認証装置3の認証側CPU31は、カード端末2xから認証側アンテナAT。及び送受信部33を順次介して起動通知データD1を受けると、ネットワークインターフェース35からネットワークNT（図1）を介してカード端末管理装置4に接続する。その後、認証側CPU31は、カード端末2xから送信される暗号化乱数パターンデータD4を認証側アンテナAT。及び送受信部33を順次介して受けると、ネットワークインターフェース35からカード端末管理装置4に送信する。

カード端末管理装置4では、この暗号化乱数パターンデータD4は、当該カード端末管理装置4に保持されている鍵情報を用いて所定の復号化処理が施され、その後に逆拡散処理が施され、カード端末2xの端末ID（シードデータD2a）が取得される。

この状態においてカード端末管理装置4では、この端末ID（シードデータD2a）が当該カード端末管理装置4に保持されているデータベースにある場合には現在の通信相手がカード端末2xであるものと判定される一方、当該データベースにない場合には現在の通信相手がカード端末2xに成りすましているものと判定され、この判定結果が管理側判定データD5として認証装置3に送信される。

またカード端末管理装置4では、カード端末2xの端末IDが、拡散データD2bに対応する拡散データで再び拡散され、当該拡散結果に対して

、カード端末 $2_x$ と同一の鍵情報を用いて暗号化処理が施され、この結果得られる暗号化乱数パターンデータ $D_6$ が認証装置 $3$ に送信される。

認証装置 $3$ の認証側CPU $3_1$ は、カード端末管理装置 $4$ から供給される管理側判定データ $D_5$ 及び暗号化乱数パターンデータ $D_6$ をネットワークインターフェース $3_5$ を介して受信し、当該管理側判定データ $D_5$ を内部メモリ $3_2$ に一時記憶すると共に、暗号化乱数パターンデータ $D_6$ を送受信部 $3_3$ 及び認証側アンテナAT $_c$ を順次介してカード端末 $2_x$ に送信する。

カード端末 $2_x$ の端末側CPU $2_1$ は、認証装置 $3$ から返信される暗号化乱数パターンデータ $D_6$ を端末側アンテナAT $_c$ 及び送受信部 $2_3$ を順次介して受けると、暗号化ノ復号化部 $2_4$ において、当該暗号化乱数バタニシデータ $D_6$ に対して鍵情報を用いて復号化処理を施し、乱数発生部 $2_5$ において、この復号化処理結果を拡散データ $D_{2b}$ により逆拡散することによってシードデータ $D_7$ を生成する。

そして端末側CPU $2_1$ は、このシードデータ $D_7$ に表される端末IDが自己的端末IDと一致した場合には現在の通信相手が認証装置 $3$ であるものと判定する一方、当該自己の端末IDと不一致であった場合には現在の通信相手が認証装置 $3$ に成りすましているものと判定し、この判定結果を端末側判定データ $D_8$ として、送受信部 $2_3$ 及び端末側アンテナAT $_c$ を順次介して認証装置 $3$ に送信する。

このようにして認証装置 $3$ の認証側CPU $3_1$ は、カード端末 $2_x$ と認証装置 $3$ とにおける相互認証に関する各種データを中継することによって、この相互認証処理結果として管理側判定データ $D_5$ と、端末側判定データ $D_8$ とをそれぞれ取得することができるよう時々なされている。

#### (1-5) 生体認証処理

次に、この生体認証処理を詳細に説明する。

実際上、認証側CPU $3_1$ は、カード端末 $2_x$ から認証側アンテナAT

。及び送受信部33を順次介して起動通知データD1を受けると、駆動制御部36を介して生体情報取得部LIRを制御し、当該生体情報取得部LIRの撮像カメラCM(図3、図4)によって、このとき近接面3A(図3、図4)に近接されるカード端末2xを持する手の指内方の血管を撮像する。

そして認証側CPU31は、バターン抽出部37において、この撮像結果として得られる血管画像信号S1に対して、A/D(Analogue/Digital)変換処理、2値化処理、血管線状化処理、分歧点等の特徴点抽出処理などの各種処理を施し、この結果得られる血管形成パターンのデータD10を認証部38に送出する。

一方、認証側CPU31は、上述のカード端末2ネと認証装置3における相互認証の中継処理の結果として、当該カード端末2x及び認証装置3から得られた端末側判定データD8及び管理側判定データD5の判定結果が相互に認証成功を表すものであった場合には、暗号化/復号化部34において、予め内部メモリ32に記憶された認証側暗号鍵D11に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された認証側暗号鍵D11を送受信部33及び認証側アンテナAT<sub>cD</sub>を順次介してカード端末2xに送信する。

カード端末2xの端末側CPU21は、この暗号化された認証側暗号鍵D11を送受信部23及び端末側アンテナAT<sub>cD</sub>を順次介して受信すると、暗号化/復号化部24において、予め内部メモリ22に記憶された端末側暗号鍵D12に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された端末側暗号鍵D12を送受信部23及び端末側アンテナAT<sub>cD</sub>を順次介して認証装置3に送信する。

また端末側CPU21は、暗号化/復号化部24において、暗号化された認証側暗号鍵D11に対して、秘密鍵を用いて所定の復号化処理を施す。そして端末側CPU21は、復号化した認証側暗号鍵D11を用いて、

内部メモリ 2 2 のEEPROMに登録された登録バターンデータ D 1 3 を  
暗号化すると共に、当該認証側暗号鍵 D 1 1 で暗号化された登録バターン  
データ D 1 3 を、端末側暗号鍵 D 1 2 を用いてさらに暗号化し、当該 2 重  
暗号化された登録バターンデータ D 1 3 を送受信部 2 3 及び端末側アンテ  
ナ A T<sub>CD</sub> を順次介して認証装置 3 に送信する。

認証装置 3 の認証側 CPU 3 1 は、暗号化された端末側暗号鍵 D 1 2 を  
認証側アンテナ A T<sub>o</sub> 及び送受信部 3 3 を順次介して受信すると、暗号  
化・復号化部 3 4 において、当該暗号化された端末側暗号鍵 D 1 2 に対し  
て、秘密鍵を用いて所定の復号化処理を施す。

また認証側 CPU 3 1 は、その後にカード端末 2 X から送信される、Z  
重暗号化された登録バターンデータ D 1 3 を待ち受ける。そして認証側 C  
PU 3 1 は、2 重暗号化された登録バターンデータ D 1 3 を受信すると、  
復号化した端末側暗号鍵 D 1 2 を用いて復号化すると共に、予め内部メモ  
リ 3 2 に記憶された認証側暗号鍵 D 1 1 を用いて復号化し、当該復号化し  
た登録バターンデータ D 1 3 を認証部 3 8 に送出するようになされている  
。

このようにして認証側 CPU 3 1 は、カード端末 2 X に登録された登録  
バターンデータ D 1 3 を取得する場合には、認証側暗号鍵 D 1 1 と、端末  
側暗号鍵 D 1 2 とをカード端末 2 X との間で相互に受け渡し、これら暗号  
鍵 D 1 1 、 D 1 2 を用いて登録バターンデータ D 1 3 を 2 重暗号化した状  
態でカード端末 2 X に送信させる。従って、この認証側 CPU 3 1 では、  
登録バターンデータ D 1 3 の送信途中での盗用を強固に防止し、セキュリ  
ティ強化を図ることができるようになされている。

認証部 3 8 は、この登録バターンデータ D 1 3 と、バターン抽出部 3 7  
で抽出された血管形成バターンのデータ D 1 0 とを照合する。そして認証  
部 3 8 は、これらデータ D 1 0 、 D 1 3 に表されるこれら血管形成バター  
ンの照合の程度が所定の閾値以上であった場合には、登録者本人であると

判定する一方、当該閾値未満であった場合には、第三者であると判定するようになされている。

#### (1-6) 認証処理手順

ここで、かかる認証側CPU31による相互認証の中継処理及び生体認証処理の一連の認証処理（以下、これを第1の認証処理と呼ぶ）は、図6に示す第1の認証処理手順RT1に従って行われる。

すなわち認証側CPU31は、近接面3Aに近接されたカード端末2xから起動通知データD1を受けると、この第1の認証処理手順RT1をステップSP0において開始し、続くステップSP1において、生体情報読み取り部LIR（図2）を起動し、当該カード端末2xを持する手の指に内在する血管形成パターンの抽出を開始する。

そして認証側CPU31は、ステップSP2において、カード端末2xと、カード端末管理サーバ4との相互認証を中継し、続くステップSP3において、当該カード端末2x及びカード端末管理サーバ4から供給される管理側判定データD5と、端末側判定データD8とに基づいて相互認証が成功したか否かを判定する。

ここで、認証側CPU31は、相互認証が成功したと判定した場合には、次のステップSP4において、自己の認証側暗号鍵D11（図5）をカード端末2xに送信すると共に、当該カード端末2xに保持された端末側暗号鍵D12（図5）をカード端末2xから取得し、続くステップSP5において、これら認証側暗号鍵D11及び端末側暗号鍵D12を用いて、カード端末2xから2重暗号化された状態で送信される登録血管形成パターンD13を復号化する。

そして認証側CPU31は、次のステップSP6において、ステップSP1で開始することにより取得したユーザの血管形成パターンと、ステップSP5で復号化した登録血管形成パターンD13に表される血管形成パターンとを照合し、続くステップSP7において、当該照合結果に基づい

て登録者本人の有無を判定した後、ステップSP8に移ってこの第1の認証処理手順RT1を終了する。

一方、認証側CPUT31は、ステップSP3で相互認証が失敗したと判定した場合には、上述のステップSP4乃至ステップSP7までの各種処理を実行することなく、ステップSP8に移ってこの第1の認証処理手順RT1を終了する。

このようにして認証側CPUT31は、第1の認証処理を実行することができるようになされている。

#### (1-7) 第1の実施の形態による動作及び効果

以上の構成において、この情報処理システム1の認証装置3は、複数のカード端末2i(図1)のうち、近接面3A(図3)に近接されたカード端末2xと通信し、当該カード端末2xに保持された登録血管形成パターンD13を取得する。

この一方で、認証装置3は、近接面3Aに近接されたカード端末2xを持持する手を撮像し、当該撮像結果から血管形成パターンを抽出する。

そして認証装置3は、これら血管形成パターンに基づいて、このとき近接面3Aにカード端末2xを近接させたユーザが、カード端末2xに保持された登録血管形成パターンの登録者であるか否かを認証する。

従ってこの認証装置3では、複数のカード端末2iにそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置3に登録する場合に比して、当該認証装置3におけるデータベースから各血管形成パターンを任意の順序で読み出して照合するといった処理を回避することができるため、当該照合時間を大幅に短縮することができる。

この場合、登録血管形成パターンはカード端末2xに保持されているため、血管形成パターンをデータベースとして認証装置3に登録する場合に比して、当該データベースに登録された血管形成パターンが認証装置3の管理者等によって盗用されるといったことを回避することができるため、

当該血管形成パターンの信頼性を向上することができるようになされている。

また認証装置3は、カード端末2xとカード端末管理サーバ4との相互認証を申継し、当該相互認証が成功したと判定した場合に生体認証を実行することにより、当該カード端末2xに保持された登録血管形成パターンを盗用して偽造カード端末に保持するといった成りすましをも回避することができるため、セキュリティの強化をより一段と図ることができる。

以上の構成によれば、複数のカード端末2iのうち、近接面3Aに近接されたカード端末2xに保持された登録血管形成パターンD13と、当該カード端末2xを持するユーザから抽出した血管形成パターンとを照合するようにしたことにより、複数のカード端末2i(図1)にそれぞれ記憶される全ての血管形成パターンをデータベースとして認証装置3に登録する場合に比して、照合処理の低減することができるため、当該照合処理の低減を通じてユーザの待ち時間を短縮化することができ、かくして使い勝手を向上することができる。

## (2) 第2の実施の形態

### (2-1) 第2の実施の形態による情報処理システムの全体構成

図7において、51は全体として第2の実施の形態による情報処理システムを示し、指輪型でなる複数の端末装置(以下、これをリング端末と呼ぶ)52i(i=1, 2, ……, N)と、認証装置53'によって構成される。

各リング端末52iは、所定のサービスの提供対象となるユーザにそれぞれ配られたものであり、固有の端末IDを、認証装置53に登録された登録血管形成パターンデータを識別するためのデータとしてそれぞれ保持している。

一方、認証装置53は、各リング端末52iにそれぞれ保持された端末IDと、登録血管パターンデータとをデータベース化して管理しており、

このデータベースの登録血管パターンデータに基づいて、サービスを受けようとするユーザが登録者本人であるか否かを判定するようになされている。なお、この情報処理システム1では、1つの認証装置3を設置する場合を例示してあるが、複数の認証装置3を所定の設置箇所に設置するようにしても良い。

この情報処理システム5.1では、サービスを提供する場合、ユーザはリング端末5.2x(x=1、2、……、又はN)を装着した部分を認証装置5.3の所定位置に近接する。この場合、認証装置5.3は、端末IDに基づいてリング端末5.2xと端末認証(相互認証)すると共に、カード端末2xを近接させた装着部分に内在する血管の血管形成パターンを取得する。

そして認証装置5.3は、端末認証(相互認証)が成功した場合には、そのカード端末2xの端末IDに基づいて、対応する登録血管パターンデータをデータベースから特定し、当該特定した登録血管パターンデータに表される血管形成パターンと、ユーザから取得した血管形成パターンを照合することによって登録者本人の有無を判定するようになされている。

とのようにしてこの情報処理システム5.1では、リング端末5.2xを認証装置5.3に近接させるだけで、当該認証装置5.3が、このときこのリング端末5.2xを装着したユーザの血管形成パターンを自動的に取得し、これをデータベースに保持された登録血管形成パターンと照合する。

この場合、認証装置5.3は、データベースに登録された複数の血管形成パターンのうち、端末認証(相互認証)で用いた端末IDに基づいて対応する登録血管形成パターンを特定してから照合するため、データベースから各血管形成パターンを任意の順序で逐一読み出して照合する場合に比して、その処理負荷を大幅に低減することができ、この結果、ユーザの待ち時間を大幅に短縮することができるようになされている。

なお、この情報処理システム5.1は、登録血管パターンデータの管理機能を認証装置5.3に設けると共に、当該管理される登録血管パターンデータ

タのなかから対応する登録血管パターンデータを識別するためのデータ（端末ID）をカード端末52iに登録させた点で、当該登録血管パターンデータの管理機能を設けることなく、個々のカード端末2iに登録血管パターンデータを登録させた情報処理システム1（図1）とは相違する。

従ってこの情報処理システム51では、情報処理システム1に比べると、認証装置53の管理者によってデータベースの登録血管パターンデータが盗用される可能性は比較的高いが、その反面、カード端末52iから登録血管パターンデータが盗用される可能性は確実になくなる。

またこの情報処理システム51は、端末認証機能及び生体認証機能を認証装置53に一括する形態となっているが、この形態は、当該端末認証機能をカード端末管理サーバ4及び生体認証機能を認証装置3に分割していた情報処理システム1（図1）の形態に比して、例えば家庭内等のように比較的小規模なシステムを構築する場合には、特に有用である。

#### （2－2）リング端末及び認証装置の構成

ここで、リング端末52x及び認証装置53の構成を説明する。

リング端末52xは、第1の実施の形態における対応部分に同一の符号を付した図8に示すように、薄厚でなる円形状のリング部54と、このリング部54の外周表面に設げられた装飾部55とからなり、当該リング部54を介して指に装着脱着することができるようになされている。

またこのリング部54の内部には、リング部54の形状に対応する端末側アンテナAT<sub>CD</sub>が収納されると共に、当該リング部54の内周表面には、複数の近赤外光光源LS（LS<sub>A</sub>～LS<sub>D</sub>）が装飾部55の近傍に配設されている。そしてこれら端末側アンテナAT<sub>CD</sub>及び近赤外光光源LSは、装飾部55の内部に収納された端末側信号処理部IC<sub>CD</sub>2に接続されている。

この端末側信号処理部IC<sub>CD</sub>2は、認証装置53から供給される電磁誘導信号を端末側アンテナAT<sub>CD</sub>を介して受信した場合、その受信に応

じて誘起される電圧を駆動電圧として起動し、予め保持された端末IDを用いて認証装置53との間で各種データ授受することによって相互認証すると共に、近赤外光光源LSを駆動制御し得るようになされている。なお、この端末側信号処理部IC<sub>UDZ</sub>の具体的な処理内容については後述する。

一方、認証装置53は、図2及び図3との対応部分に同一符号を付した図9及び図10に示すように、第1の実施の形態における認証装置3に比して、近接面3Aに設けられた近赤外光光源LSを省いた点（ただし、端末側に新たに設けられている）と、認証側信号処理部IC<sub>1</sub>に代えて認証側信号処理部IC<sub>2</sub>を設げた点を除いて、第1の実施の形態における認証装置3と同一構成となっている。

具体的に認証側信号処理部IC<sub>2</sub>は、認証側信号処理部IC<sub>1</sub>における相互認証中継処理に代えて、リング端末52xと直接的に相互認証する相互認証処理を設けた点と、当該認証側信号処理部IC<sub>1</sub>における生体認証処理に代えて、登録者本人の有無を2手法を用いて判定する生体認証処理（以下、これを2重生体認証処理と呼ぶ）を設げた点が相違点となっている。

かかる相互認証処理及び2重生体認証処理を、図5との対応部分に同一符号を付した図11を用いて詳細に説明する。

#### (2-3) 相互認証処理

リング端末52xの端末側CPU61は、認証装置3から供給される電磁誘導信号を端末側アンテナAT<sub>CD</sub>を介して受信した場合、その受信に応じて誘起される電圧を駆動電圧として起動する。そして端末側CPU61は、第1の実施の形態で上述したように、起動通知データD1を端末側アンテナAT<sub>OD</sub>及び送受信部23を順次介して認証装置53に送信した後、暗号化乱数パターンデータD4を生成して認証装置53に送信する。

認証装置3の認証側CPU71は、リング端末52xから供給される起

動通知データD1を認証側アンテナAT。及び送受信部33を順次介して受けると、その後にリング端末52xから供給される暗号化乱数パターンデータD4を待ち受ける。

認証側CPU71は、暗号化乱数パターンデータD4を受けた場合、暗号化ノ復号化部34において、予め保持されたカード端末2xと同一の鍵情報を用いて所定の復号化処理を施した後、乱数発生部72において、当該復号結果に対して逆拡散処理を施し、この結果得られるリング端末52xの端末ID（シードデータD2a）を取得する。

この状態において認証側CPU71は、この端末IDがハードディスク73におけるデータベースにある場合には現在の通信相手がリング端末52xであるものと判定する一方、当該データベースにない場合には現在の通信相手がリング端末52xに成りすましているものと判定し、当該判定結果を管理側判定データD5として内部メモリ32に一時的に記憶する。

また認証側CPU71は、乱数発生部72において、リング端末52xにおける拡散データD2bに対応する拡散データで再び端末IDを拡散した後、暗号化ノ復号化部34において、当該拡散結果に対して、鍵情報を用いて暗号化処理を施し、この結果得られる暗号化乱数パターンデータD6を送受信部33及び認証側アンテナAT。を順次介してリング端末52xに送信する。

すなが端末52xの端末側CPU61は、この暗号化乱数パターンデータD6に対して第1の実施の形態と同様にして各種処理を施し、この結果得られるシードデータD7に表される端末IDが自己の端末IDと一致した場合には現在の通信相手が認証装置53であるものと判定する一方、当該自己の端末IDと不一致であった場合には現在の通信相手が認証装置53に成りすましているものと判定し、この判定結果を端末側判定データD8として、送受信部23及び端末側アンテナAT<sub>cD</sub>を順次介して認証装置53に送信する。

このようにして認証装置 5 3 の認証側 C P U 7 1 は、リング端末 5 2 x との間における端末認証（相互認証）結果として管理側判定データ D 5 と、端末側判定データ D 8 をそれぞれ取得することができるようになされている。

#### （2－4）生体認証処理

次に、2重生体認証処理について説明する。

実際上、認証側 C P U 7 1 は、リング端末 5 2 x から供給される起動通知データ D 1 を受けた場合に、シードデータ D 2 0 a 及び拡散データ D 2 0 b を生成する。そして認証側 C P U 7 1 は、暗号化ノ復号化部 3 4 において、シードデータ D 2 0 a 及び拡散データ D 2 0 b に対して、予め保持している鍵情報を用いて所定の暗号化処理を施し、当該暗号化されたシードデータ D 2 0 a 及び拡散データ D 2 0 b を送受信部 3 3 及び認証側アンテナ A T<sub>D</sub> を順次介してリング端末 5 2 x に送信する。

一方、リング端末 5 2 x の端末側 C P U 6 1 は、暗号化されたシードデータ D 2 0 a 及び拡散データ D 2 0 b を端末側アンテナ A T<sub>C\_D</sub> 及び送受信部 2 3 を順次介して受けると、暗号化ノ復号化部 2 4 において、当該暗号化されたシードデータ D 2 0 a 及び拡散データ D 2 0 b に対して復号化処理を施す。

そして端末側 C P U 6 1 は、乱数発生部 2 5 において、復号化したシードデータ D 2 0 a を拡散データ D 2 0 b により拡散し、近赤外光光源 L<sub>S</sub> の点灯を表す「1」と近赤外光光源 L<sub>S</sub> の非点灯を表す「0」とからなる点滅パターンのデータ（以下、これを点滅パターンデータと呼ぶ） D 2 1 を生成する。

この状態において端末側 C P U 6 1 は、光源駆動部 6 2 において、点滅パターンデータ D 2 1 に基づいて近赤外光光源 L<sub>S</sub> を点滅させると共に、暗号化ノ復号化部 2 4 において、当該点滅パターンデータ D 2 1 に対して、秘密鍵を用いて暗号化処理を施し、当該暗号化された点滅パターンデータ D 2 1 を生成する。

タ D 2 1 を送受信部 2 3 及び端末側アンテナ A T<sub>CD</sub> を順次介して認証装置 5 3 に送信する。

認証側 C P U 7 1 は、リング端末 5 2 x から、暗号化された点滅パターンデータ D 2 1 を認証側アンテナ A T 及び送受信部 3 3 を順次介して受けた場合、暗号化ノ復号化部 3 4 において、当該暗号化された点滅バターンデータ D 2 1 を復号化し、この結果得られる点滅バターンデータ D 2 1 を点滅パターン照合部 7 6 に送出する。

また認証側 C P U 7 1 は、撮像カメラ C M も制御し、このとき近接面 3 A (図 1 0) に近接されるリング端末 5 2 x を装着する指内方の血管を撮像するようになされている。

ここで、この実施の形態の場合、リング端末 5 2 x を装着する手と、近接面 3 A とは所定の位置関係を保つて近接するようになされており、例えば、図 1 0 に示したように、所定の指背に装飾部 5 5 が対向するようにリング端末 5 2 x を装着し、当該指の指腹を、近接面 3 A に対して平行となる状態かつ所定方向 D R から対向させた状態で近接するようになされている。

なお、この近接面 3 A に対して手を能動的に近接するようにしても良く、あるいは、所定の位置に配置させるための部材(図示せず)を介して受動的に近接するようにしても良い。

このようにしてリング端末 5 2 x を装着する手を近接面 3 A に近接させた場合。図 1 2 において破線で示すように、当該リング端末 5 2 x の近赤外光光源 L S から発射される近赤外光は、そのリング端末 5 2 x を装着する指に照射され、当該指に内在する血管を通るヘモグロビンに吸収されると共に血管以外の組織で散乱及び反射してその指から出射する。この出射した近赤外光は、血管投影光として得られ、この血管投影光が、開口窓 0 W から撮像カメラ C M の撮像レンズ 1 0 a、絞り(図示せず)及び近赤外光透過フィルタ 1 0 b を順次介して固体撮像素子 1 0 c に入射し、血管画

像信号  $S_{10j}$  ( $J = 1, 2, \dots, m$ ) として輝度パターン生成部 74 及びパターン抽出部 75 に送出される。

輝度パターン生成部 74 は、血管画像信号  $S_{10j}$  における輝度状態の変化を検出する。ここで、血管画像信号  $S_{10j}$  における輝度状態は、近赤外光光源  $L_S$  の点滅パターンに対応するものとなっているため、当該近赤外光光源  $L_S$  が非点灯のときには暗い状態となり、これに対して近赤外光光源  $L_S$  が点灯のときには明るい状態となっている。

そして輝度パターン生成部 74 は、かかる検出結果に基づいて、血管画像信号  $S_{10j}$  における輝度状態が明るい状態を表す「1」と当該輝度状態が暗い状態を表す「0」とからなるパターン（以下、これを輝度パターンと呼ぶ）データ  $D_{30}$  を生成し、これをパターン抽出部 75 及び点滅パターン照合部 76 に送出する。

パターン抽出部 75 は、撮像カメラ CM から供給される血管画像信号  $S_{10j}$  に対して A/D (Analog/Digital) 変換処理や血管線状化処理等の各種処理を施した後に 2 値化処理を施し、2 値血管画像のデータを生成する。

そしてパターン抽出部 75 は、輝度パターン生成部 76 から供給される輝度パターンデータ  $D_{30}$  に基づいて、これら 2 値血管画像のデータのなかから近赤外光光源  $L_S$  の点灯時に対応する 1 枚の 2 値血管画像を選択し、当該選択した 2 値血管画像から分岐点等の特徴点抽出し、この結果得られる血管形成パターンのデータ  $D_{10}$  を認証部 77 に送出する。

点滅パターン照合部 76 は、リング端末 52X から供給された点滅パターンデータ  $D_{21}$  と、輝度パターン生成部 74 から供給される輝度パターンデータ  $D_{30}$  との状態（「1」及び「0」の配列状態）を照合することによって、例えば血管形成パターンのフィルムに近赤外光を照射する等といったような巧妙な成りすまし行為を検出するようになされている。

そして点滅パターン照合部 76 は、かかる照合結果が一致した場合には

成りすまし行為がないものと判定する一方、当該照合結果が不一致であつた場合には成りすまし行為があるものと判定し、この判定結果を点滅パターン判定データD31として認証部77に送出する。

一方、認証側CPU71は、上述のリング端末52xとの間ににおける相互認証により得た端末側判定データD8及び認証側判定データD5の判定結果が相互に認証成功を表すものであつた場合には、暗号化／復号化部34において、予め内部メモリ32に記憶された認証側暗号鍵D11に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された認証側暗号鍵D11を送受信部33及び認証側アンテナAT。を順次介してリング端末52xに送信する。

リング端末52xの端末側CPU61は、この暗号化された認証側暗号鍵D11を送受信部23及び端末側アンテナAT<sub>CD</sub>を順次介して受信すると、暗号化／復号化部24において、予め内部メモリ22に記憶された端末側暗号鍵D12に対して、秘密鍵を用いて所定の暗号化処理を施し、当該暗号化された端末側暗号鍵D12を送受信部23及び端末側アンテナAT<sub>CD</sub>を順次介して認証装置53に送信する。

また端末側CPU61は、暗号化／復号化部24において、暗号化された認証側暗号鍵D11に対して、秘密鍵を用いて所定の復号化処理を施す。そして端末側CPU61は、復号化した認証側暗号鍵D11を用いて、内部メモリ22のEEPROMに記憶された端末IDを暗号化すると共に、当該認証側暗号鍵D11で暗号化された端末IDを、端末側暗号鍵D12を用いてさらに暗号化し、当該2重暗号化された端末IDを送受信部23及び端末側アンテナAT<sub>CD</sub>を順次介して認証装置53に送信する。

認証装置53の認証側CPU71は、暗号化された端末側暗号鍵D12を認証側アンテナAT。及び送受信部33を順次介して受信すると、暗号化／復号化部34において、当該暗号化された端末側暗号鍵D12に対して、秘密鍵を用いて所定の復号化処理を施す。

また認証側 C P U 7 1 は、その後に リング端末 S 2 X から送信される、2重暗号化された端末 I D を待ち受ける。そして認証側 C P U 7 1 は、2重暗号化された端末 I D を受信すると、復号化した端末側暗号鍵 D 1 2 を用いて復号化すると共に、予め内部メモリ 3 2 に記憶された認証側暗号鍵 D 1 1 を用いて復号化し、当該復号化した端末 I D を認証部 7 7 に送出するようになされている。

このようにして認証部 7 7 には、かかる端末 I D と、点滅パターン照合部 7 6 から供給される点滅パターン判定データ D 3 1 と、パターン抽出部 7 5 から供給される血管形成パターンのデータ D 1 0 とがそれぞれ入力されることとなる。

認証部 7 7 は、点滅パターン判定データ D 3 1 の判定結果が成りすまし行為がない旨を表している場合には、端末 I D に対応する登録血管形成パターンデータをデータベースから検索し、当該端末 I D に対応する登録血管形成パターンデータ五 D をハードディスク 7 3 から読み出す。

そして認証部 7 7 は、ハードディスク 7 3 から読み出した登録血管形成パターンデータ R D と、パターン抽出部 7 5 から供給される血管形成パターンのデータ D 1 0 に基づいて、登録者本人の有無を判定するようになされている。

#### (2-5) 認証処理手順

ここで、かかる認証側 C P U 7 1 による相互認証処理及び2重生体認証処理の一連の認証処理（以下、これを第2の認証処理と呼ぶ）は、図13に示す第2の認証処理手順 R T 2 に従って行われる。

すなわち認証側 C P U 7 1 は、近接面 3 A に近接されたカード端末 2 X から起動通知データ D 1 （図11）を受けると、この第2の認証処理手順 R T 2 をステップ S P 1 0 において開始し、続くステップ S P 1 1 において、リング端末 S 2 X と相互認証処理を実行し、続くステップ S P 1 2 において、当該相互認証処理結果として得られる管理側判定データ D 5 と、

端末側判定データD8に基づいて相互認証が成功したか否かを判定する。  
。

ここで、認証側CPU71は、相互認証が成功したと判定した場合には、次のステップSP13において、所定のシードデータD20a及び拡散データD20b(図11)を暗号化した状態でリング端末52xに送信する。この場合、リング端末52xでは、これらシードデータD20a及び拡散データD20bに基づいて点滅パターンデータD21(図11)が生成され、当該点滅パターンデータD21が暗号化された状態で認証装置53に送出されると共に、その点滅パターンデータD21に基づいて近赤外光光源LS(図12)が点滅される。

次いで、認証側CPU71は、ステップSP14において、撮像カメラCM(図12)を起動し、当該撮像カメラCMでの撮像結果(血管撮像信号S10j)に基づいて、リング端末52xを持する手の指に内在する血管形成パターンを抽出する。

そして認証側CPU71は、次のステップSP15において、リング端末52xから送信される点滅パターンデータD21に表される点滅パターンと、撮像カメラCMで撮像された血管撮像信号S10jにおける輝度パターンとを照合し、続くステップSP16において、当該点滅パターン及び輝度パターンが一致すると判定した場合には、ステップSP17に移る。  
。

認証側CPU71は、このステップSP17において、ステップSP11での相互認証時に得られるリング端末52xの端末IDに対応付けられた登録血管形成パターンデータRDをデータベースから特定し、当該端末IDに対応する登録血管形成パターンデータRDをハードディスク73から読み出す。

そして認証側CPU71は、次のステップSP18において、この登録血管形成パターンデータRDに表される血管形成パターンと、ステップS

P 1 4 でユーザから抽出した血管形成パターンとを照合し、続くステップ S P 1 9において、当該照合結果に基づいて登録者本人の有無を判定した後、次のステップ S P 2 0に移ってこの第2の認証処理手順 R T 2 を終了する。

一方、認証側 C P U 7 1 は、ステップ S P 1 2 で相互認証が失敗したと判定した場合、又はステップ S P 1 6 で点滅パターン及び輝度パターンが一致しないと判定した場合には、当該ステップ S P 1 9 で登録者本人の有無を判定するまでもなく、当該登録者以外の第三者からのアクセスであるため、その後の各種処理を実行せずにステップ S P 2 0 に移ってこの認証処理手順 R T 2 を終了する。

このようにして認証側 C P U 7 1 は、第2の認証処理を実行することができるようになされている。

#### (2-6) 第2の実施の形態による動作及び効果

以上の構成において、この情報処理システム 5 1 の認証装置 5 3 は、複数のリング端末 5 2 i (図7) のうち、近接面 3 A (図10) に近接されたリング端末 5 2 x と通信して相互認証し、当該リング端末 5 2 x に保持された端末 ID を取得する。

そして認証装置 5 3 は 相互認証が成功した場合には、この端末 ID に対応する登録血管形成パターンデータ R D に表される血管形成パターンと、血管画像信号 S 1 0 J から抽出した血管形成パターンとを照合し、登録者の有無を判定する。

従って、この認証装置 5 3 では、当該認証装置 3 におけるデータベースから各血管形成パターンを任意の順序で逐一読み出して照合するといった処理を回避することができるため、当該照合時間を大幅に短縮することができる。

またこの認証装置 5 3 は、相互認証の一方で、近接面 3 A に近接されたリシグ端末 5 2 x を装着する手に対して、所定の点滅パターンでリンク端

末 5 2 x の近赤外光光源 L S を点滅させると共に、当該手を撮像する。そして認証装置 5 3 は、相互認証が成功した場合には、近赤外光光源 L S を点滅させた点滅パターンと、撮像結果として得られる血管画像信号 S 1 0 j の輝度パターンとを照合し、当該照合結果に応じて、血管形成パターンに基づく登録者の有無を判定する。

従ってこの認証装置 5 3 では、第三者による登録者への成りすましを異なる観点から 2 重にチェックできるため、巧妙な成りすましを回避することができ、セキュリティの強化をより二段と図ることができる。

以上の構成によれば、相互認証により得られる端末 I D を登録血管形成パターンデータの識別子として、複数の登録血管形成パターンデータのなかから対応する登録血管形成パターンデータ R D を特定し、当該登録血管形成パターンデータ R D に表される血管形成パターンと、血管画像信号 S 1 0 j から抽出した血管形成パターンとに基づいて登録者の有無を判定するようにしたことにより、データベースから各血管形成パターンを任意の順序で逐一読み出して照合するといった処理を回避してその照合処理の低減することができるため、当該照合処理の低減した分だけユーザの待ち時間を短縮化することができ、かくして使い勝手を向上することができる。

### (3) 他の実施の形態

上述の第 1 の実施の形態では端末側（カード端末 2 i）に登録血管形成パターンデータを登録し、第 2 の実施の形態では認証側（認証装置 5 3）に登録血管形成パターンデータを登録し、当該登録された血管形成パターンと、ユーザから抽出した血管形成パターンとが一致したときに登録者と判定するようにした場合について述べたが、本発明はこれに限らず、図 2 及び図 5 との対応部分に同一符号を付した図 1 4 に示すように、当該端末装置 1 0 2 x 及び端末 I D を管理する端末管理サーバ 1 0 4 の双方に登録血管形成パターンデータを登録し、当該登録された 2 つの血管形成パターンと、認証装置 1 0 3 によってユーザから抽出された血管形成パターンと

の3つがそれぞれ一致したときに登録者と判定するようにも良い。

この図14に示す情報処理システム101では、第三者は、互いに異なる箇所にそれぞれ登録される登録血管形成パターンデータそれぞれを盗用することは困難であることから、当該登録された登録血管形成バターンデータの一方を第三者のものにすりかえたとしてもこれを検出することができ、この結果、セキュリティの強化をより一段と図ることができる。

なお、この端末装置102xは、カード形状又はリング形状のいずれであっても良く、これ以外の形状であっても携帯型のものであれば、他の種々の形状のものを適用することができる。また、近赤外光光源LSは、第1の実施の形態のように認証側に設けられていても良く、第2の実施の形態のように端末側に設けられていても良い。

ここで、かかる認証装置103の認証処理手順を、図15に示すフローチャートを用いて説明する。

すなねち認証側CPU131は、近接面3Aに近接された端末装置102xから起動通知データD1を受けると、この第3の認証処理手順RT3をステップSP20において開始し、続くステップSP21において、撮像カメラCM(図2)を起動し、このときこの端末装置102xを把持又は装着している手(指)に内在する血管形成パターンの抽出を開始する。

そして認証側CPU131は、ステップSP22において、端末装置102xと、端末管理サーバ104との相互認証を中継し、続くステップSP23において、当該端末装置102x及び端末管理サーバ104から供給される管理側判定データD5と、端末側判定データD8に基づいて相互認証が成功したか否かを判定する。

この相互認証が成功したと判定した場合、認証側CPU131は、次のステップSP24において、自己の認証側暗号鍵D11(図5)を端末装置102xに送信すると共に、当該端末装置102xに保持された端末側暗号鍵D12(図5)を端末装置102xから取得し、続くステップSP

25において、これら認証側暗号鍵D11及び端末側暗号鍵D12を用いて、端末装置102xから2重暗号化された状態で送信される登録血管形成パターンD13を復号化する。

また認証側CPU131は、ステップSP26において、ステップSP24及びSP25の各種処理と同様にして、端末IDと登録血管形成パターンとの対応付をデータベースとして管理する端末管理サーバ104と暗号鍵を相互に交換し、当該端末管理サーバ104の暗号鍵及び認証装置103の認証側暗号鍵D11を用いて、2重暗号化された状態で送信される登録血管形成パターンD13を復号化する。ちなみにこの登録血管形成パターンD13は、端末管理サーバ104に登録される複数の登録血管形成パターンのうち、相互認証時に用いられた端末IDに対応するものである。

そして認証側CPU131は、次のステップSP27に括いて、ステップSP21で開始することにより取得したユーザの血管形成パターンPT1(図14)と、ステップSP25で端末装置102xから取得した登録血管形成パターンD13に表される血管形成パターンPT2(図14)と、ステップSP26で端末管理サーバ104から取得した登録血管形成パターンD13に表される血管形成パターンPT3(図14)とを照合し、続くステップSP28において、当該照合結果に基づいて登録者本人の有無を判定した後、ステップSP29に移ってこの第3の認証処理手順RT3を終了する。

一方、ステップSP23で相互認証が失敗したと判定した場合、認証側CPU131は、上述のステップSP24乃至ステップSP28までの各種処理を実行することなく、ステップSP29に移ってこの第3の認証処理手順RT3を終了する。

このようにしてこの認証装置103は、端末装置102x及び端末管理サーバ104に登録された登録血管形成パターンデータと、認証装置10

3 によってユーザから抽出された血管形成パターンとに基づいて登録者の有無を判定することができる。

なお、登録者の有無の判定機能を端末管理サーバ 1 0 4 に設けるようにしても、端末装置 1 0 2 X 及び端末管理サーバ 1 0 4 に登録された登録血管形成パターンデータと、認証装置 1 0 3 によってユーザから抽出された血管形成パターンとを、当該端末管理サーバ 1 0 4 に集めるようすれば、上述の第 3 の認証処理手順 R T 3 と同様の手順で三者相互間の生体認証を実現できる。

また、別の例として、図 1 4 との対応部分に同一符号を付した図 1 6 に示すように、登録対象の端末装置 1 0 2 X 及び端末管理サーバ 1 0 4 には、登録血管形成パターンデータを登録しておき、管理機能を有する端末管理サーバ 1 0 4 には、当該登録血管形成パターンデータに対応付けて、登録血管形成パターンデータを生成するまでの処理過程のデータから生成したハッシュ値を登録しておく。

そして、認証装置 1 0 3 は、端末装置 1 0 2 X 及び端末管理サーバ 1 0 4 に登録された登録血管形成パターンデータを取得し、当該登録血管形成パターンデータに表される血管形成パターン P T 2 、 P T 3 同士を照合する。その一方で、認証装置 1 0 3 は、このとき端末管理サーバ 1 0 4 から取得した登録血管形成パターンデータに対応するハッシュ値 H 1 も取得し、このハッシュ値 H 1 と、ユーザから抽出した血管形成パターンのデータを生成するまでの処理過程のデータから生成したハッシュ値 H 2 とを照合する。

このようにすれば、第三者は、登録血管形成パターンデータを盗用するのみならず、ハッシュ値生成アルゴリズムや、ハッシュ値 H 2 がいずれの処理過程で得られたデータを用いて生成したかを知らなければ、成りすましができないことになるため、セキュリティの強化をより一段と図ることができる。

また、登録血管形成パターンデータと、ユーザから抽出した血管形成パターンのデータとを照合する場合に比して、データ量が少ない分だけ照合処理負荷を低減することができる、ユーザの待ち時間をより一段と短縮化することができる。

なお、この場合、認証側 C P U 1 3 1 は、図 1 5 との対応部分に同一符号を付した図 1 7 に示す第 4 の認証処理手順 R T 4 のように、第 3 の認証処理手順 R T 3 におけるステップ S P 2 6 及び S P 2 7 に代えて、当該ステップ S P 2 6 及び S P 2 7 での取得対象及び照合対象を一部変更したステップ S P 2 6' 及び S P 2 7' を設けるだけで、当該第 3 の認証処理手順 R T 3 と同様の処理手順に従って生体認証処理を実行することができる。

さらに、別の例として、図 2 及び図 5 との対応部分に同一符号を付した図 1 8 に示す情報処理システム 2 0 1 を適用することもできる。この情報処理システム 2 0 1 では、所定の秘密鍵を用いて暗号化された暗号登録血管形成パターンデータ D 1 0 0 が端末装置 2 0 2 x に登録され、当該未暗号化状態における登録血管形成パターンデータのハッシュ値 H 1 と、秘密鍵 K Y とが端末 I D に対応付けられて端末管理サーバ 2 0 4 に登録される。

この端末装置 2 0 2 x は、カード形状又はリング形状のいずれであっても良く、これ以外の形状であっても携帯型のものであれば、他の種々の形状のものを適用することができる。また、近赤外光光源 L S は、第 1 の実施の形態のように認証側に設けられていても良く、第 2 の実施の形態のように端末側に設げられていても良い。

認証装置 2 0 3 は、この端末装置 2 0 2 x を近接された場合に、当該端末装置 2 0 2 x を把持又は装着している手（指）に内在する血管形成パターンの抽出を開始する。一方で、認証装置 2 0 3 は、暗号登録血管形成パターンデータ D 1 0 0 を端末装置 2 0 2 x から取得すると共に、当該端末

装置202xの端末IDに対応する登録血管形成パターンデータのハッシュ値H1と、秘密鍵KYとを端末管理サーバ204から取得する。

そして認証装置203は、所定のアルゴリズムに従って、秘密鍵KYを用いて暗号登録血管形成パターンデータD100を復号化すると共に、当該復号化された登録血管形成パターンデータからハッシュ値を生成し、当該生成したハッシュ値（以下、これを比較用ハッシュ値と呼ぶ）と、端末管理サーバ204から取得したハッシュ値H1とを照合する。

また認証装置203は、この照合結果が一致した場合には、ユーザから取得した血管形成パターンPTと、復号化した登録血管形成パターンデータに表される血管形成パターンとを照合する。

このようにこの情報処理システム201では、暗号登録血管形成パターンデータD100に対して個別の秘密鍵KYは端末装置202xに送られないため、この秘密鍵KYが分からなければ、第三者には暗号登録血管形成パターンデータD100から比較用ハッシュ値を式めることは不可能となる。従って、この情報処理システム201においては、端末装置202x内の暗号登録血管形成パターンデータD100を置き換えた場合には、一般に、ハッシュ値を用いた最初の照合段階で第三者であることを判定することができるため、登録血管形成パターンを用いて照合する場合に比して、データ量が少ない分だけ照合処理負荷を大幅に低減することができ、ユーザの待ち時間をより一段と短縮化することができる。

またこの情報処理システム201においては、第三者は、互いに異なる箇所にそれぞれ登録される暗号登録血管形成パターンデータD100、秘密鍵KY及びハッシュ値H1を盗用することは困難であると共に、これら暗号登録血管形成パターンデータD100及び秘密鍵KYから比較用ハッシュ値を求めることが困難であるため、端末装置202x内の暗号登録血管形成パターンデータD100を置き換えたとしてもこれを検出することができ、この結果、セキュリティの強化をより一段と図ることができる。

これに加えてこの情報処理システム201においては、登録血管形成パターンデータそのものを管理することができないため、外部に対する血管形成パターンの流出等を防止でき、より一段とセキュリティを強化することができる。

さらにこの情報処理システム201においては、登録血管形成パターンデータそのものを管理することができないため、当該登録血管形成パターンデータを管理することによる処理負荷を回避できると共に、その管理する登録血管形成パターンデータの送信処理を回避することができるため、全体として処理パフォーマンスを向上することができる。

ここで、かかる認証装置203の認証処理手順を、図19に示すフローチャートを用いて説明する。

すなねち認証側CPU231は、近接面3Aに近接された端末装置202Xから起動通知データD1を受けると、この第5の認証処理手順RT5をステップSP30において開始し、続くステップSP31において、撮像カメラCM(図2)を起動し、このときこの端末装置202Xを把持又は装着している手(指)に内在する血管形成バターンの抽出を開始する。

そして認証側CPU231は、ステップSP32において、端末装置202Xと、端末管理サーバ204との相互認証を中継し、続くステップSP33において、当該端末装置202X及び端末管理サーバ204から供給される管理側判定データD5と、端末側判定データD8に基づいて相互認証が成功したか否かを判定する。

この相互認証が成功したと判定した場合、認証側CPU231は、次のステップSP34において、自己の認証側暗号鍵D11(図5)を端末装置202Xに送信すると共に、当該端末装置202Xに保持された端末側暗号鍵D12(図5)を端末装置202Xから取得し、続くステップSP35において、これら認証側暗号鍵D11及び端末側暗号鍵D12を用いて、端末装置202Xから2重暗号化された状態で送信される暗号登録血

管形成パターンD100(図18)を復号化する。

また認証側CPU231は、ステップSP36において、ステップSP34及びSP35の各種処理と同様にして、端末管理サーバ204と暗号鍵を相互に交換し、当該端末管理サーバ204の暗号鍵及び認証装置203の認証側暗号鍵D11を用いて、2重暗号化された状態で送信される秘密鍵KY及びハッシュ値H1(図18)を復号化する。ちなみにこの秘密鍵KY及びハッシュ値H1は、端末管理サーバ204に登録される複数の秘密鍵及びハッシュ値のうち、相互認証時に用いられた端末IDに対応するものである。

そして認証側CPU231は、次のステップSP37において、この秘密鍵KYを用いて、ステップSP35で端末装置202Xから取得した暗号登録血管形成パターンデータD100を復号化すると共に、当該復号化された登録血管形成パターンデータから比較用ハッシュ値を生成し、ステップSP38に移る。

認証側CPU231は、このステップSP38において、ステップSP37で生成した比較用ハッシュ値と、ステップSP36で端末管理サーバ204から取得したハッシュ値H1とを照合し、これらが一致しない場合には、ステップSP37で復号化した登録血管形成パターンデータに表される血管形成パターンと、ステップSP31で開始することにより取得したユーザの血管形成パターンPT(図18)とを照合し、続くステップSP39において、当該照合結果に基づいて登録者本人の有無を判定した後、ステップSP40に移ってこの第5の認証処理手順RT5を終了する。

一方、ステップSP33で相互認証が失敗したと判定した場合、認証側CPU231は、上述のステップSP34乃至ステップSP39までの各種処理を実行することなく、ステップSP40に移ってこの第5の認証処理手順RT5を終了する。

このようにしてこの認証装置203は、互いに異なる箇所にそれぞれ登

録される暗号登録血管形成パターンデータD100、秘密鍵KY及びハッシュ値H1に基づいて三者相互間の生体認証を実現できる。

なお、登録者の有無の判定機能を端末管理サーバ204に設けるようにしても、端末装置202Xに登録された暗号登録血管形成パターンデータD100と、認証装置203によってユーザから抽出された血管形成パターンPTとを、当該端末管理サーバ204に集めるようすれば、上述の第5の認証処理手順RT5と同様の手順で三者相互間の生体認証を実現できる。

さらに上述の実施の形態では、登録血管形成パターンデータを電磁誘導方式により送信するデータ送信処理と、当該登録血管形成パターンデータに基づく生体認証処理との具体的な関係については述べなかつたが、本発明は、これら処理を図20に示すような関係で行うようとする。

すなねちこの図20(A)に示すように、端末側は、送信対象の登録血管形成パターンデータD13を所定単位で分割し、当該分割したデータD<sub>13k</sub>(k=1、2、3、……、1)を順次送信する。一方、認証側は、送信されたデータD<sub>13k</sub>順に、当該データD<sub>13k</sub>と、登録血管形成パターンデータD13の対応するデータ部分とを照合する(生体認証処理)。

ここで、認証側は、例えば図20(B)に示すように、通信エラーによりデータD<sub>132</sub>を受信できなかつた場合には、生体認証処理を中断すると共に、再度データD<sub>132</sub>から送信すべき旨を端末側に通知する。その後、認証側は、再びデータD<sub>132</sub>から順次送信されることに、当該データD<sub>13k</sub>と、登録血管形成パターンデータD13の対応するデータ部分とを照合する。

このようにすれば、通信エラーが生じるたびに、登録血管形成パターンデータD13の送信及び照合を最初からやりなおす場合に比して、当該送信処理及び照合処理の負荷を低減することができ、ユーザの待ち時間をよ

り一段と短縮化することができる。

さらに上述の実施の形態においては、カード状の端末装置（第1の実施の形態におけるカード端末2*i*）又は指に装着可能な端末装置（第2の実施の形態におけるリング端末5*2i*）を適用するようにした場合について述べたが、端末側信号処理部IC<sub>CD</sub>1又はIC<sub>CD</sub>2（図2、図8等）と、端末側アンテナAT<sub>CD</sub>（図2、図8等）とが搭載された腕輪、ネックレス、イヤリング、眼鏡等の付属品を適用するようにしても良い。また端末側信号処理部IC<sub>CD</sub>1又はIC<sub>CD</sub>2（図2、図8等）と、端末側アンテナAT<sub>CD</sub>（図2、図8等）とが搭載された携帯電話機、PDA（Personal Digital Assistants）等の携帯型電子機器に適用するようにしても良い。要は、携帯型のものであれば、これを端末装置として採用することができる。

さらに上述の実施の形態においては、生体における識別対象として指に内在する血管を適用するようにした場合について述べたが、本発明はこれに限らず、例えば生体に内在する神経や、生体に表在する指紋、あるいは声紋や口紋等、この他種々の生体識別対象を適用することができる。因みに、神経を認証対象とする場合には、例えば神経に特異的なマーカを体内に注入し、当該マーカを撮像するようすれば、上述の実施の形態と同様にして神経を認証対象とすることができる。

この場合、生体センサとして上述の実施の形態では血管を撮像する撮像カメラCMを採用したが、本発明はこれに限らず、適用する生体識別対象に対応するものを適宜採択することができる。また、生体識別対象をパターンとして抽出する手法も、適用する生体識別対象に対応する手法を適宜採択することができる。なお、識別対象として血管を適用する場合に、上述の実施の形態とは異なる構成の生体センサを採択するようにしても良く、パターン抽出部の内容を適宜取捨選択するようにしても良い。

さらに上述の実施の形態においては、登録血管形成パターンデータ又は

端末 ID を未暗号化状態で端末側の内部メモリ 22 に登録するようにした場合について述べたが、本発明はこれに限らず、当該暗号化した状態において内部メモリ 22 に登録しておくようにしても良い。

さらに上述の実施の形態においては、登録血管形成パターンデータと、ユーザから取得した血管形成パターンのデータとを照合する認証部 38 又は 77 を認証装置 3 又は 53 に設けるようにした場合について述べたが、本発明はこれに限らず、当該認証装置 3 又は 53 に代えて、ユーザの血管パターンを抽出する抽出装置を設げると共に、その抽出装置に対してインターネット等の所定のネットワークを介して認証サーバを設げ、当該認証サーバに認証部 38 の機能を搭載するようにしても良い。これにより、認証装置 3 又は 53 の盗難等による個人データの流出等を未然かつ有効に防止することができ、また認証サーバに登録血管形成パターンデータを一括して格納することにより、登録血管形成パターンデータや認証部の管理等を簡素化することができる。

さらに上述の実施の形態においては、生体認証処理を実行する前に、相互認証処理を実行するようにした場合について述べたが、本発明はこれに限らず、当該相互認証処理を実行する前に、生体認証処理を実行するようにしても良い。なお、この場合、生体認証処理で用いるためのユーザから抽出する血管形成パターンデータについては、かかる生体認証処理及び相互認証処理の過程での種々のタイミングで抽出することができる。

さらに上述の第 2 の実施の形態においては、近赤外光光源 LS を点滅させた点滅パターンと、撮像結果として得られる血管画像信号 S10j の輝度パターンとを照合し、当該照合結果に応じて、血管形成パターンに基づく登録者の有無を判定するようにした場合について述べたが、本発明はこれに限らず、当該判定機能を情報処理システム 1 (図 1) 又は情報処理システム 101 (図 14) に適用するようにしても良い。なお、この場合、近赤外光光源 LS を点滅させる点滅パターンデータについては、認証側に

おげるシードデータD20a及び拡散データD20bから端末側で生成するようにしたが、予め点滅パターンデータを端味側で保持しても良い。

さらに上述の第2の実施の形態においては、複数の端末IDに対応づけられた登録血管形成パターンデータをハードディスク73に格納した場合について述べたが、本発明はこれに限らず、この他種々のハードディスク以外の記録媒体に記録することができ、またハードディスクに代えてインターネット等の所定のネットワークを介して認証サーバを設け、当該認証サーバに登録血管形成パターンデータを格納するようにしても良い。

さらに上述の第2の実施の形態においては、端末IDに対応する登録血管形成パターンデータをデータベースから特定した場合について述べたが、本発明はこれに限らず、この他種々の固有となる識別子に登録血管形成パターンデータを対応付け、当該識別子に基づいてデータベースから登録血管形成パターンデータを特定するようにしても良い。

#### 産業上の利用可能性

本発明は、携帯品を用いるユーザにおける登録者の有無を判定する場合に利用可能である。

## 請求の範囲

1. 第1の情報処理装置と、第2の情報処理装置とによって構成される情報処理システムにおいて、

上記第1の情報処理装置は、

生体の所定部位における識別対象を生体識別データとして記憶する記憶手段と、

上記生体に保持されて所定の位置にまで近接され、当該位臍に近接された状態で通信する第1の通信手段と

を具え、

上記第2の情報処理装置は、

上記位置に近接された上記生体を生体データとして検出する生体センサと、

上記位置に近接された上記生体に保持される上記第1の通信手段と通信する第2の通信手段と、

上記生体センサで検出された上記生体データから上記所定部位に対応する生体データを抽出する抽出手段と、

上記抽出手段で抽出された上記所定部位に対応する生体データと、上記第1及び第2の通信手段を介んで上記第1の情報処理装置から取得した上記生体識別データとに基づいて生体認証する生体認証手段と

を具えることを特徴とする情報処理システム。

2. 所定の位置に近接された生体を生体データとして検出する生体センサと、

上記位置に近接された上記生体に保持される通信対象と通信する近距離通信手段と、

上記生体センサで検出された上記生体データから上記所定部位における生体データを抽出する抽出手段と、

上記抽出手段で抽出された上記所定部位における生体データと、上記通信対象に登録され、当該通信対象から上記近距離通信手段を介して取得した上記生体識別データとに基づいて照合する生体認証手段と  
を具えることを特徴とする情報処理装置。

3. 上記通信対象を管理する管理サーバに対して所定のネットワークを介して通信するネットワーク通信手段と、

上記本ネットワーク通信手段及び上記近距離通信手段を介して上記通信対象と、上記管理サーバとの相互認証を中継する中継手段とをさ弓に見え、  
上記相互認証の結果に応じて上記生体認証手段による照合が行われ、又は上記生体認証手段による照合結果に応じて上記中継手段による上記相互認証の中継が行われる

ことを特徴とする請求項2に記載の情報処理装置。

4. 上記通信対象に登録された上記生体識別データを対応付けて管理する管理サーバに対して所定のネットワークを介して通信するネットワーク通信手段をさらに見え、

上記生体認証手段は、

上記抽出手段で抽出された上記所定部位における生体データと、上記ネットワーク通信手段を介して上記管理サーバから取得した上記生体識別データと。上記近距離通信手段を介して上記通信対象から取得した上記生体識別データとを相互に照合する

ことを特徴とする請求項2に記載の情報処理装置。

5. 上記通信対象に登録された上記生体識別データと、当該生体識別データを生成するまでの過程で得られるデータを用いて圧縮データとを対応付けて管理する管理サーバに対して所定のネットワークを介して通信するネットワーク通信手段とをさらに見え、

上記抽出手段は、

上記生体センサで検出された上記生体データから上記所定部位における

生体データを抽出するまでの過程で得られるデータを用いて圧縮データを生成し、

上記生体認証手段は、

上記抽出手段で生成された上記圧縮データと、上記ネットワーク通信手段を介して上記管理サーバから取得した上記圧縮データとを照合することを特徴とする請求項2に記載の情報処理装置。

6. 上記生体認証手段は、

上記抽出手段で生成された上記圧縮データと、上記ネットワーク通信手段を介して上記管理サーバから取得した上記圧縮データとを照合すると共に、上記抽出手段で抽出された抽出された上記所定部位に安げる生体データと、上記近距離通信手段を介して上記通信対象から取得した上記生体識別データとを照合する

ことを特徴とする請求項5に記載の情報処理装置。

7. 上記生体に保持される上記通信対象には、光源が設けられ、

上記光源に対する点滅状態を制御する点滅パターンを生成する生成手段と、

上記生成手段において生成された上記点滅パターンを暗号化する暗号化手段と

をさらに具え、

上記生体認証手段は、

上記点滅パターンと、上記位置に近接された上記通信対象における上記光源から上記点滅パターンに従つて点滅照射され、当該位置に近接された上記生体を介して上記生体センサで検出された上記生体データの輝度パターンとを照合する

ことを特徴とする請求項2に記載の情報処理装置。

8. 上記生体識別データは、所定の分割単位のデータとしてそれぞれ分割され、

上記生体認証手段は、

上記分割単位のデータを取得することに、上記所定部位における生体データの対応するデータ部分と生体認証し、当該分割単位のデータを取子守できなかつた場合には、その取得できなかつた分割単位のデータから再耳傳を開始する

ことを特徴とする請求項 2 に記載の情報処理装置。

9. 生体の所定部位に装着する装着手段と、

上記所定部位における識別対象を生体識別データとして記憶する記憶手段と、

上記装着手段に保持され、当該装着手段を装着した上記所定部位を近接させた通信対象に対して上記生体識別データを送信する通信手段と  
を具え、

上記通信対象では、上記装着手段を装着した状態で近接された上記生体が生体データとして検出される

ことを特徴とする情報処理装置。

10. 上記通信対象から供給される信号の受信に応じて誘起する電圧蓄積する電圧蓄積手段を具え、

上記通信手段は、

上記電圧蓄積手段により蓄積された電圧を起電力として、上記通信対象に対して上記生体識別データを送信する

ことを特徴とする請求項 9 に記載の情報処理装置。

11. 上記装着手段は、

円形状のリング部ヒ、

上記リング部に設けられ、上記所定部位における識別対象に撮像光哀照射する光源とかなり、

上記撮像光は、

上記通信対象に近接された上記生体を介して、当該通信対象に設け弓れ

た撮像素子に導光される

ことを特徴とする請求項 9 に記載の情報処理装置。

12. 上記撮像光は、上記通信対象から供給される点滅パターンに従って点滅照射し、

上記点滅パターンは、上記撮像光に基づいて順次生成される画像の輝度パターンと比較される

ことを特徴とする請求項 9 に記載の情報処理装置。

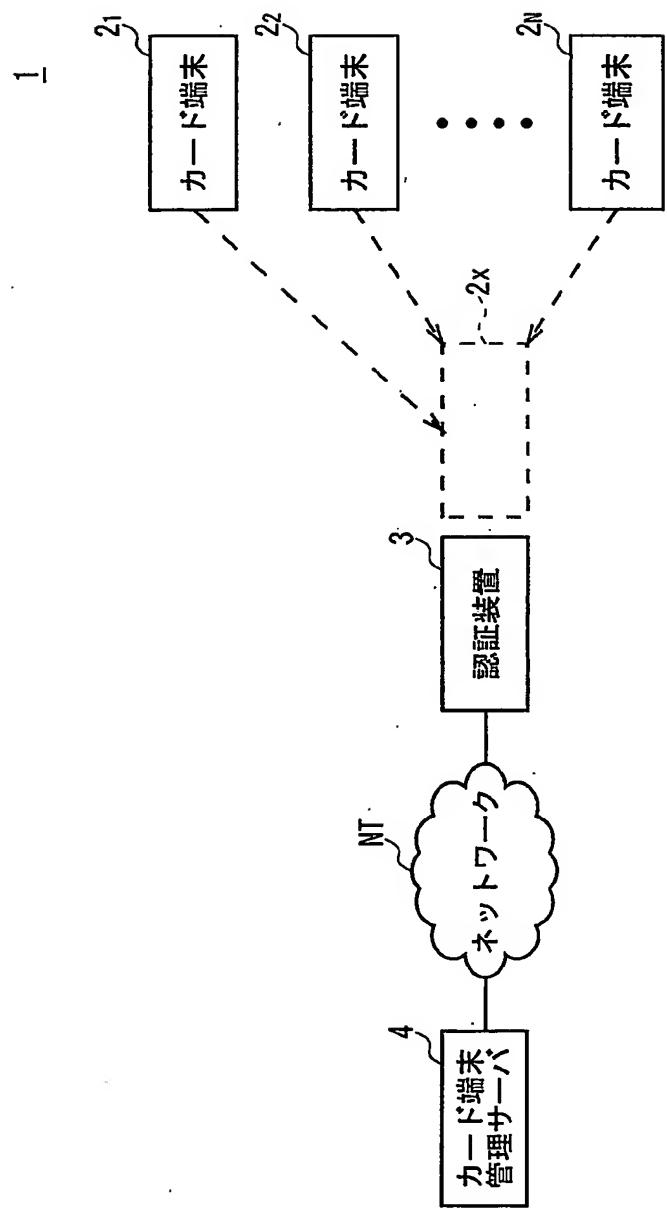


図 1

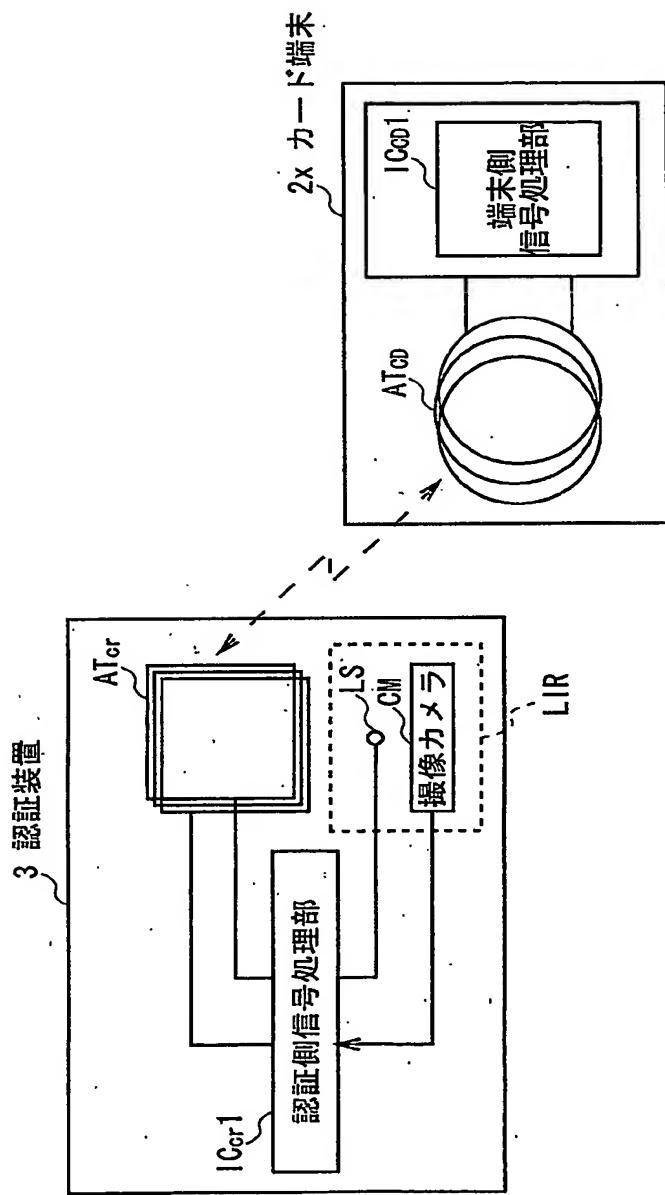


図2

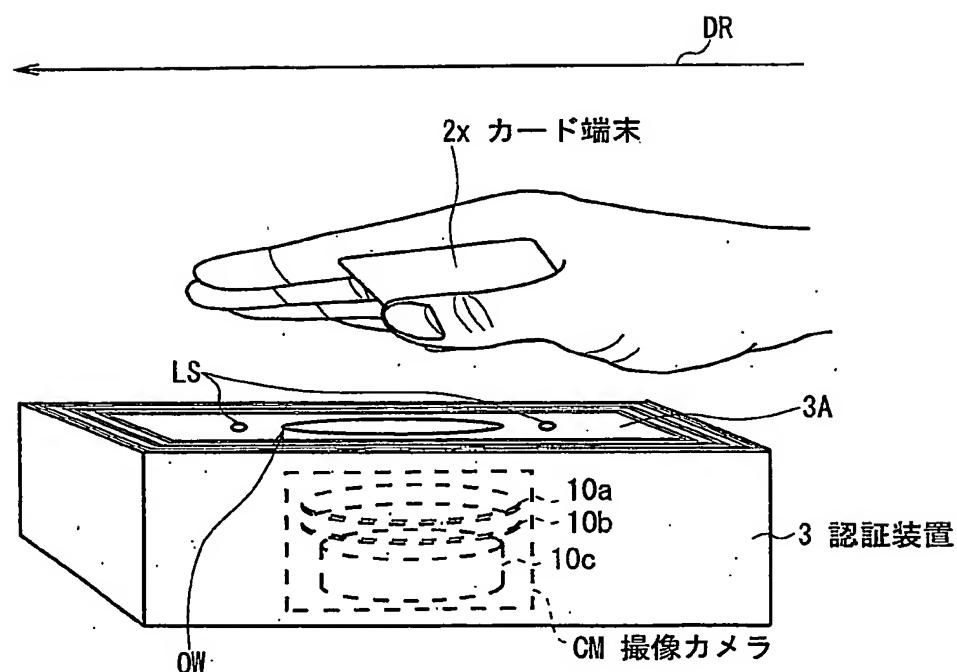


図 3

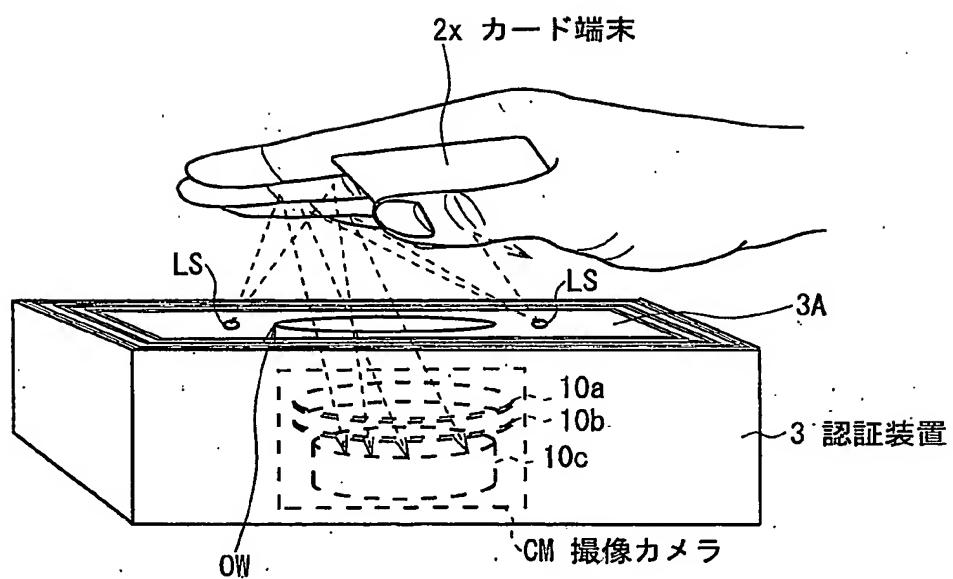


図 4

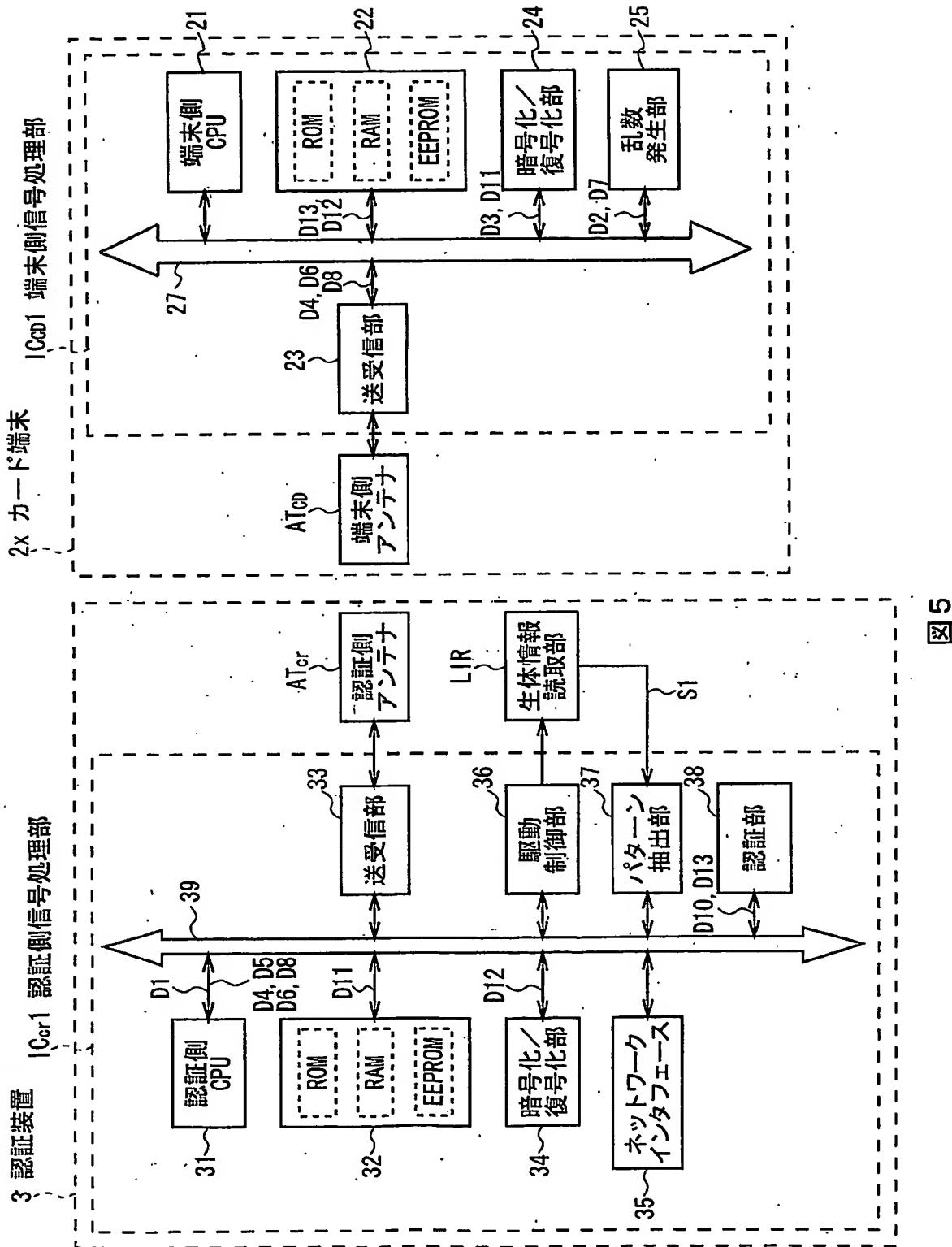


図5

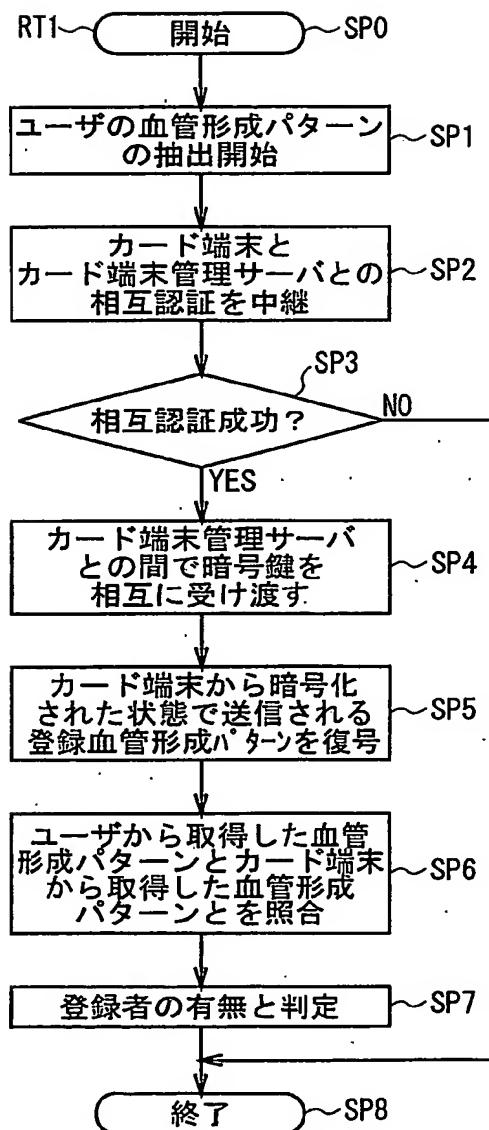


図 6

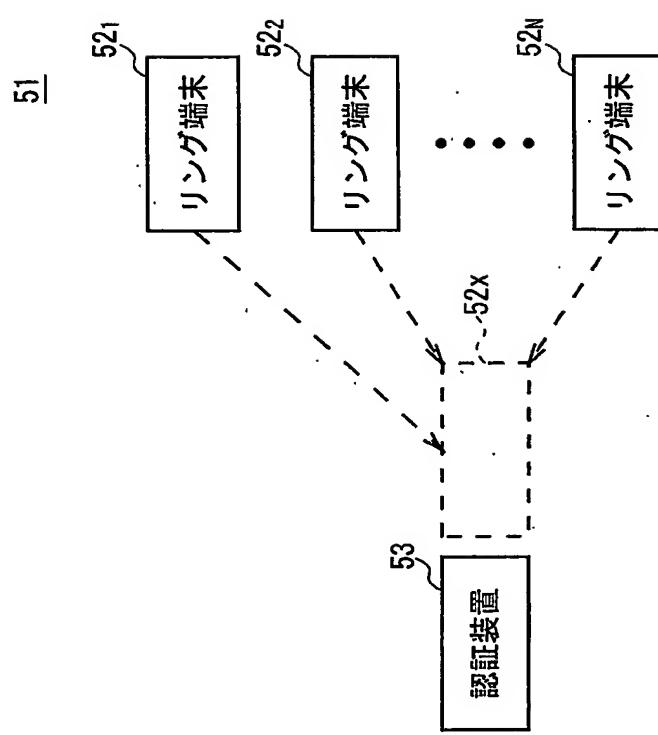


図7

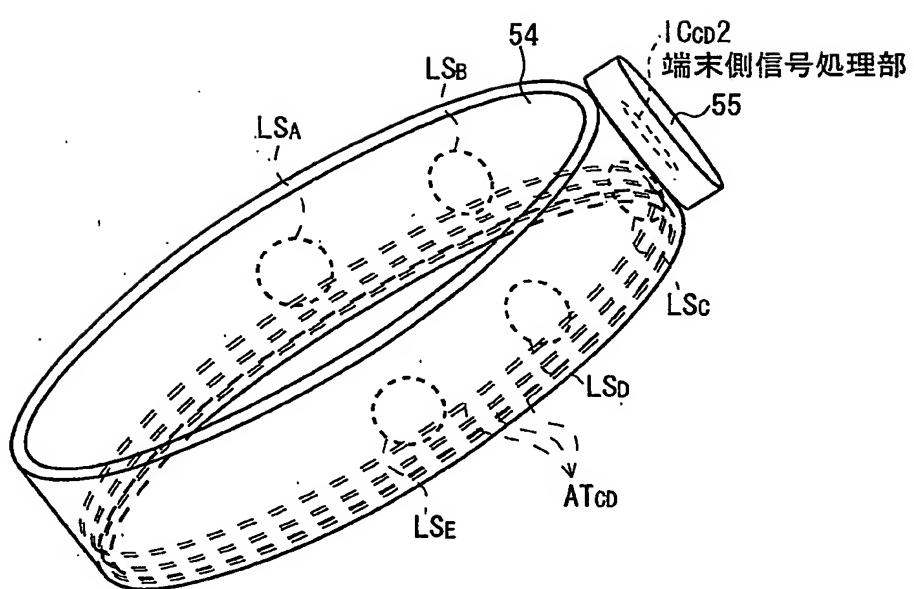
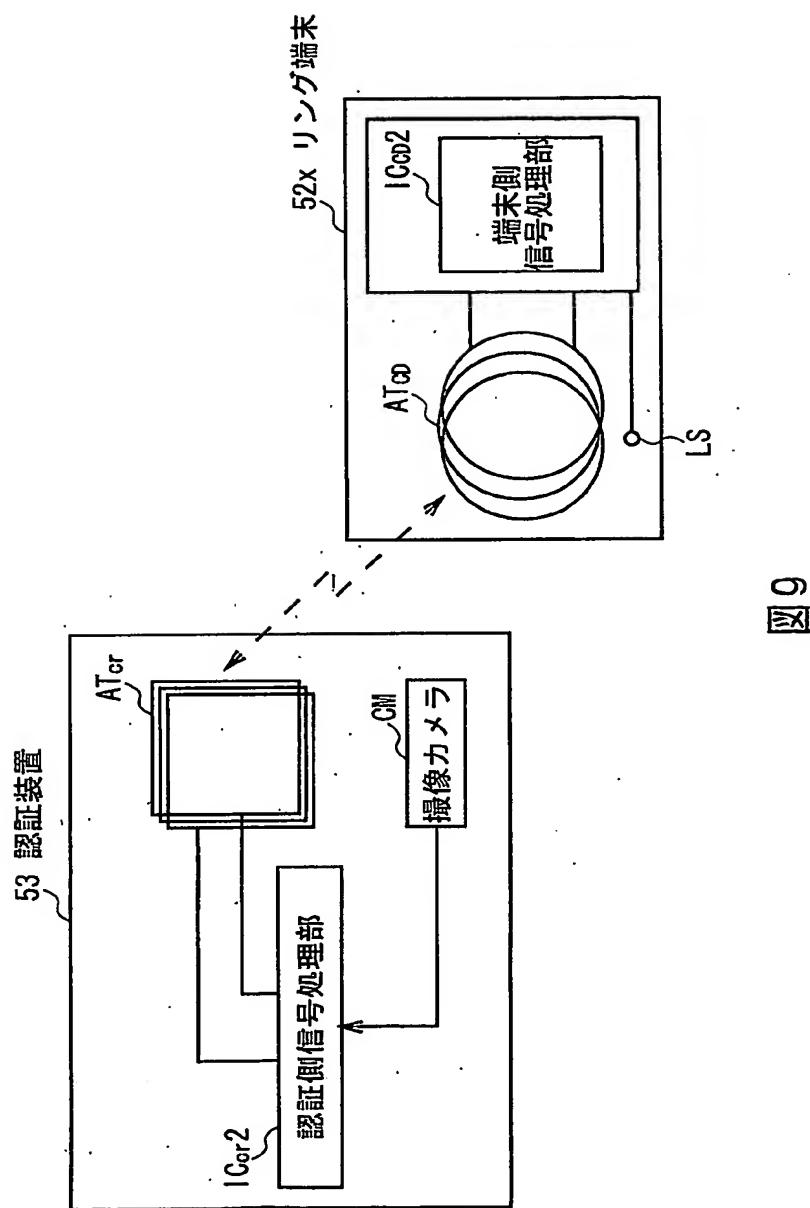


図 8



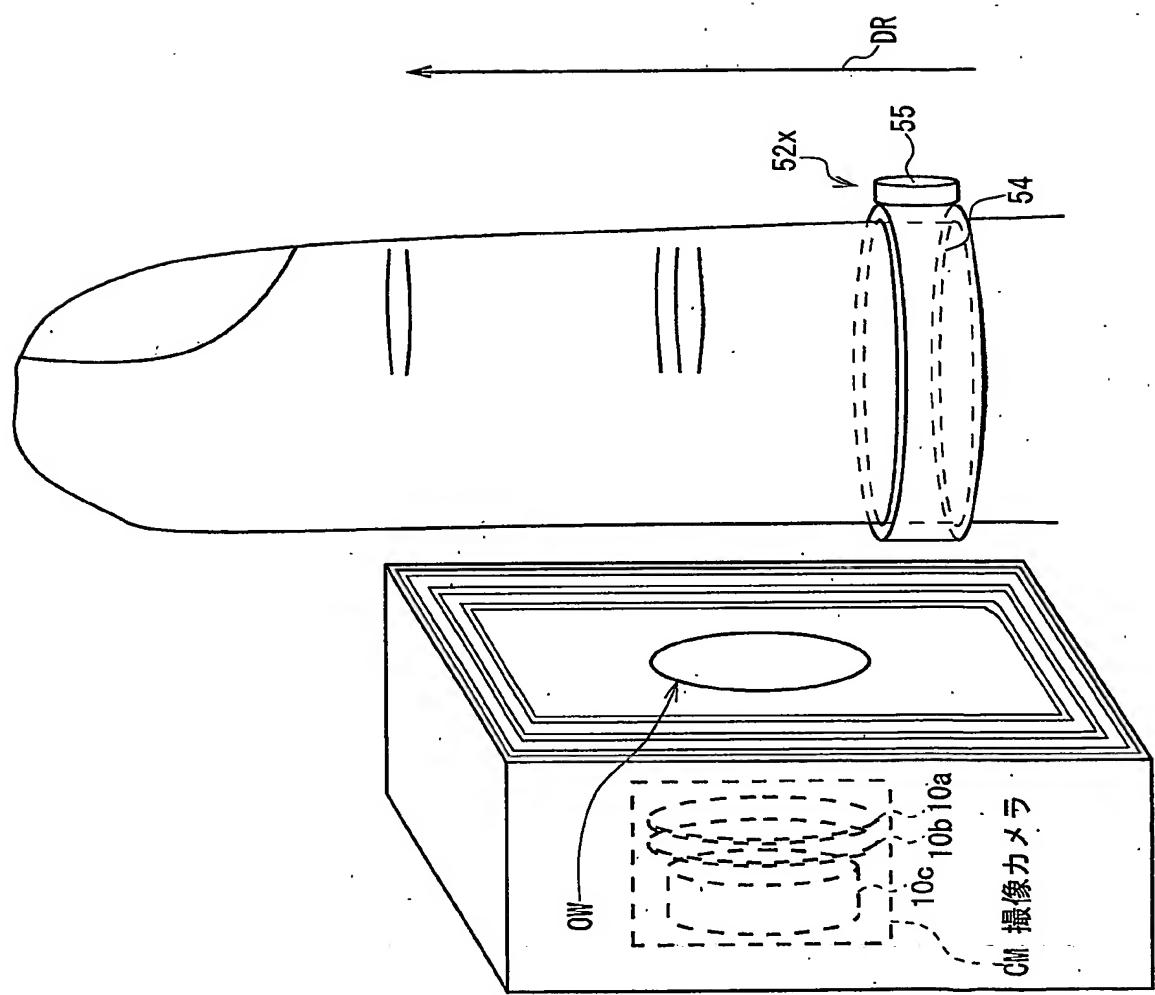
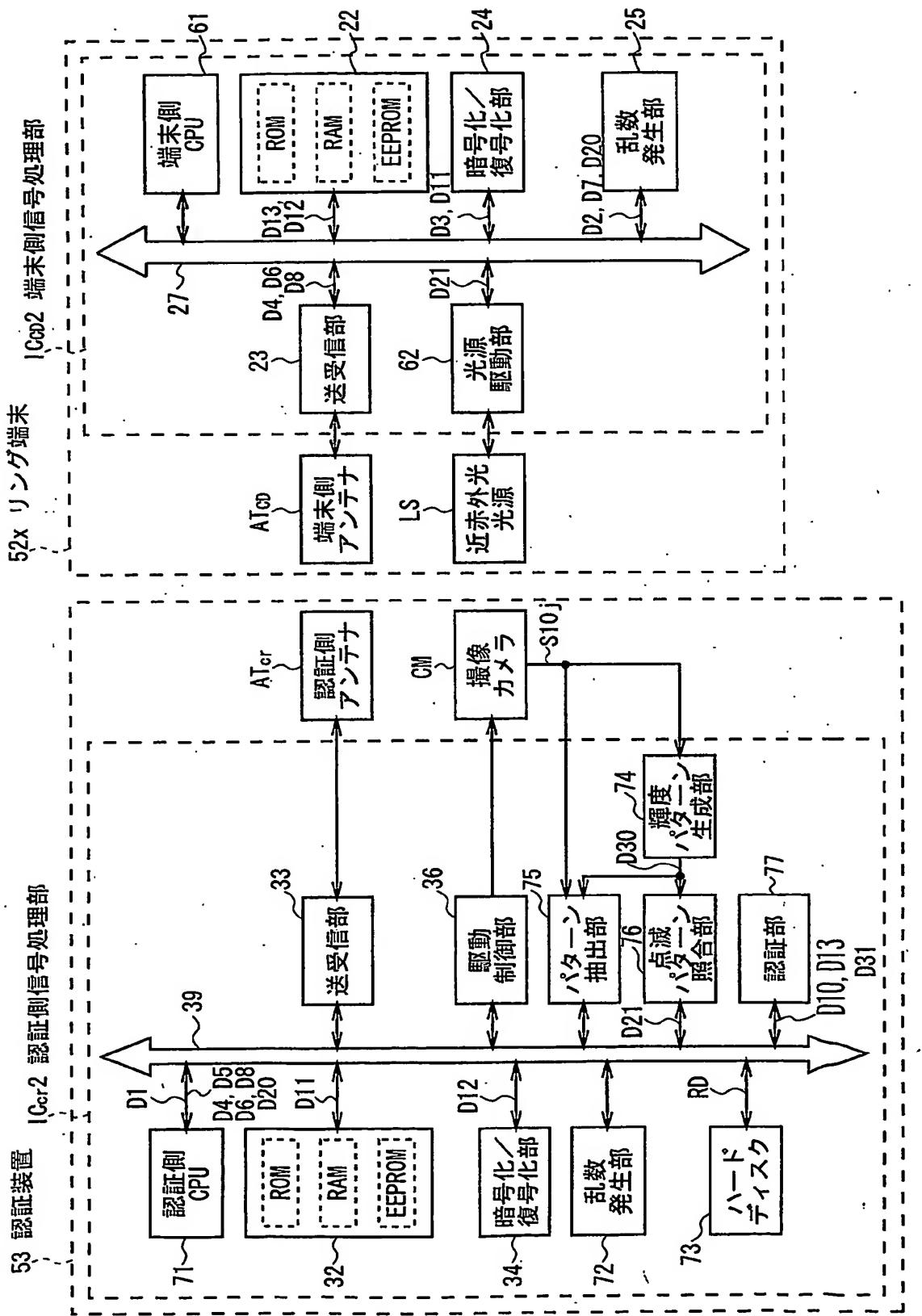


図10



一  
一  
四

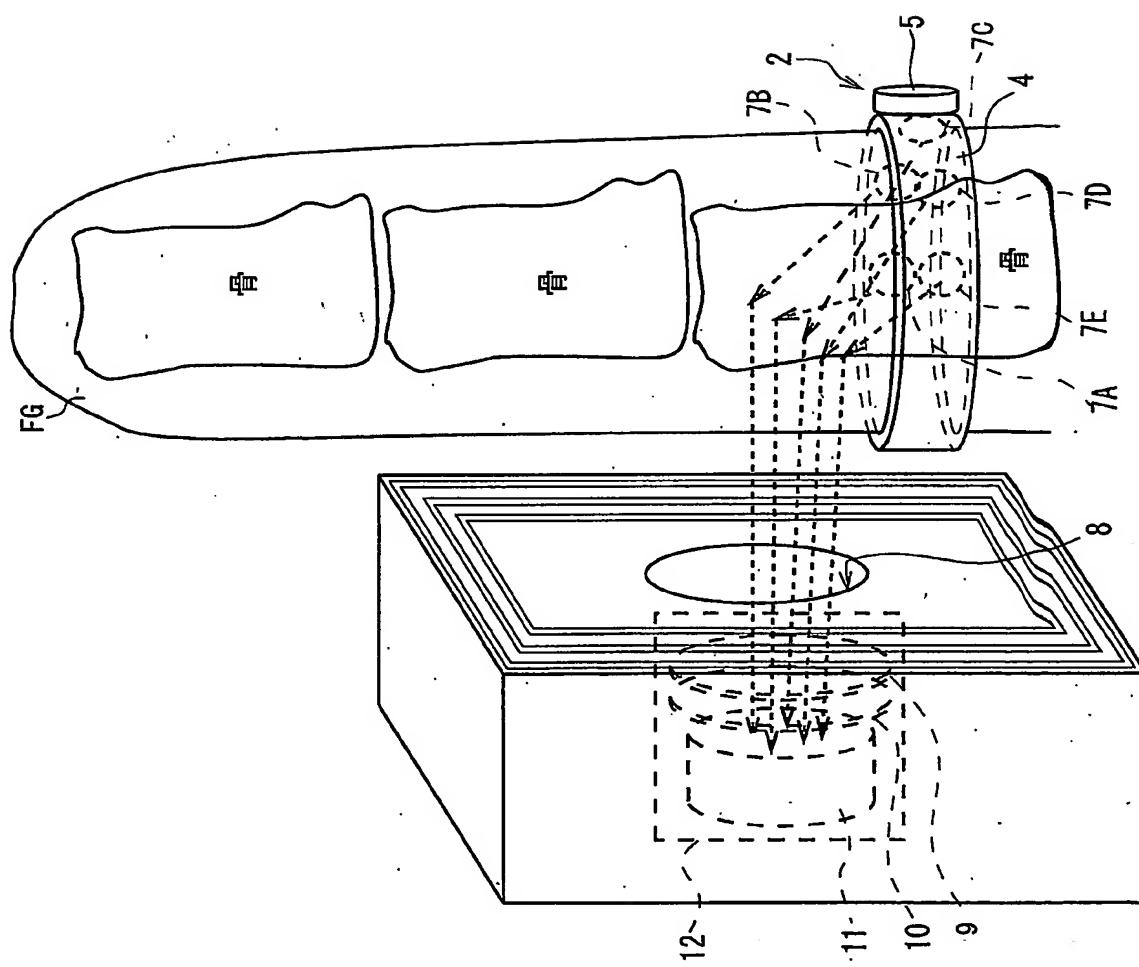


図12

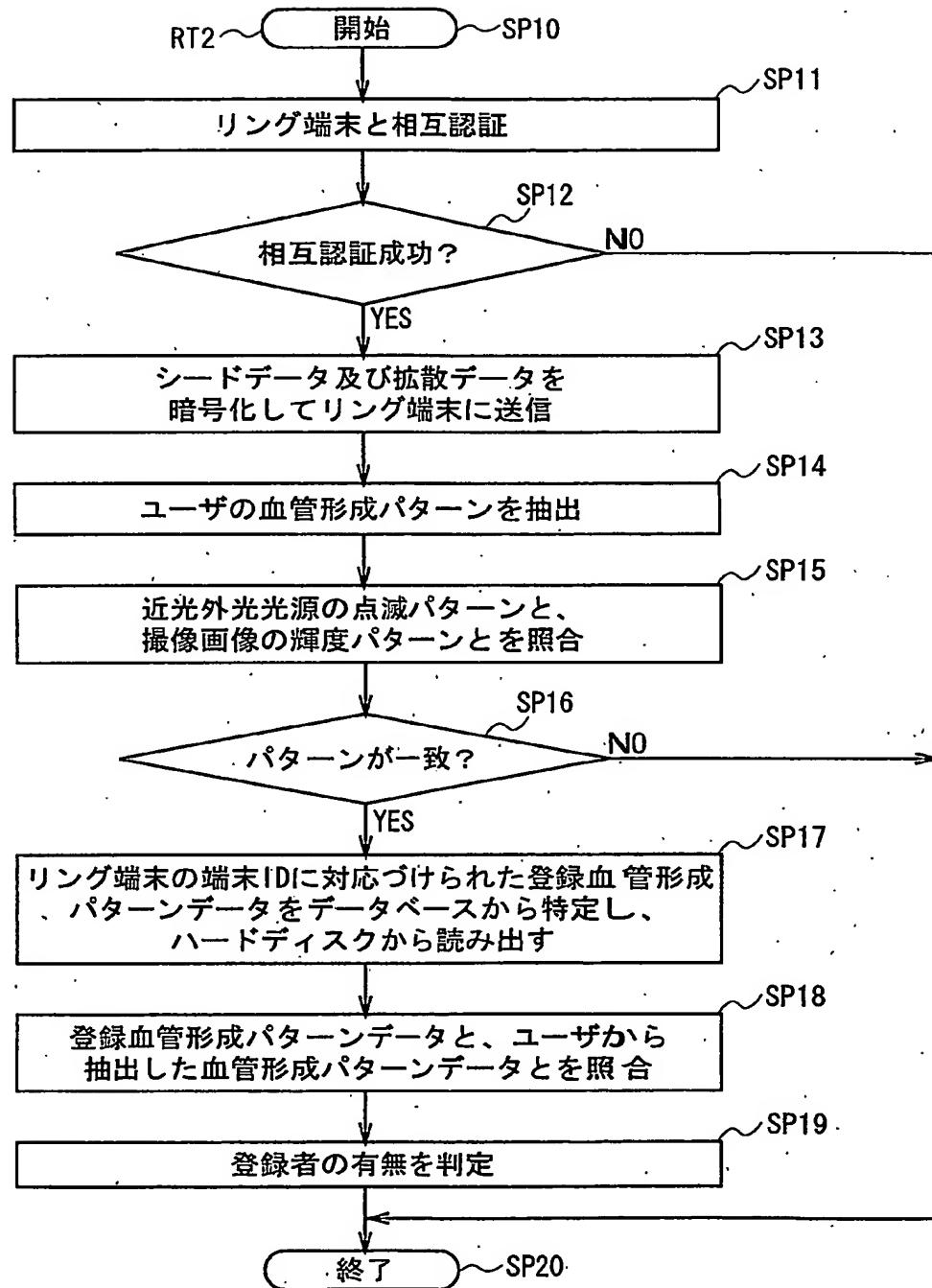


図 13

103 認証装置  
101

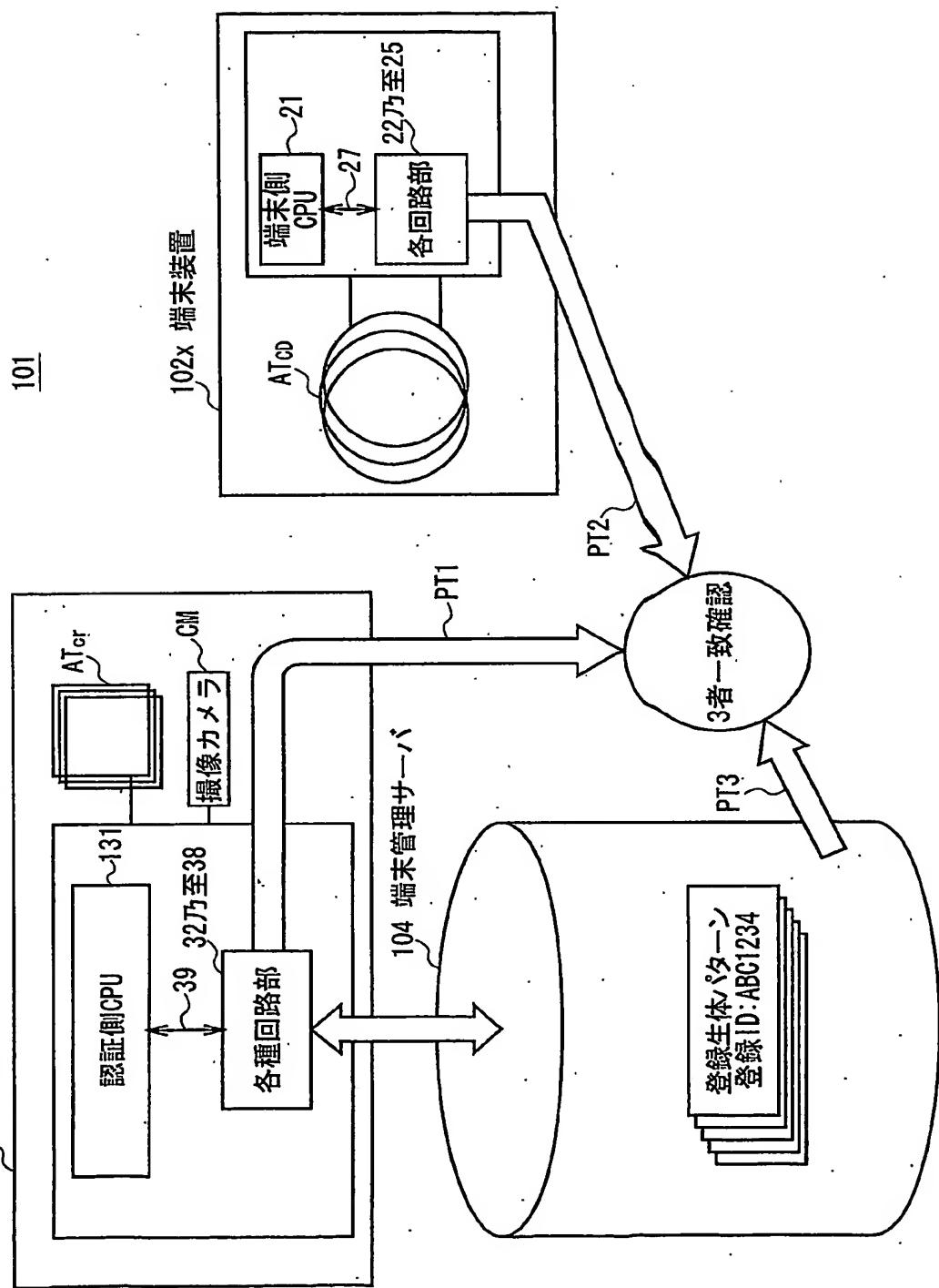


図14

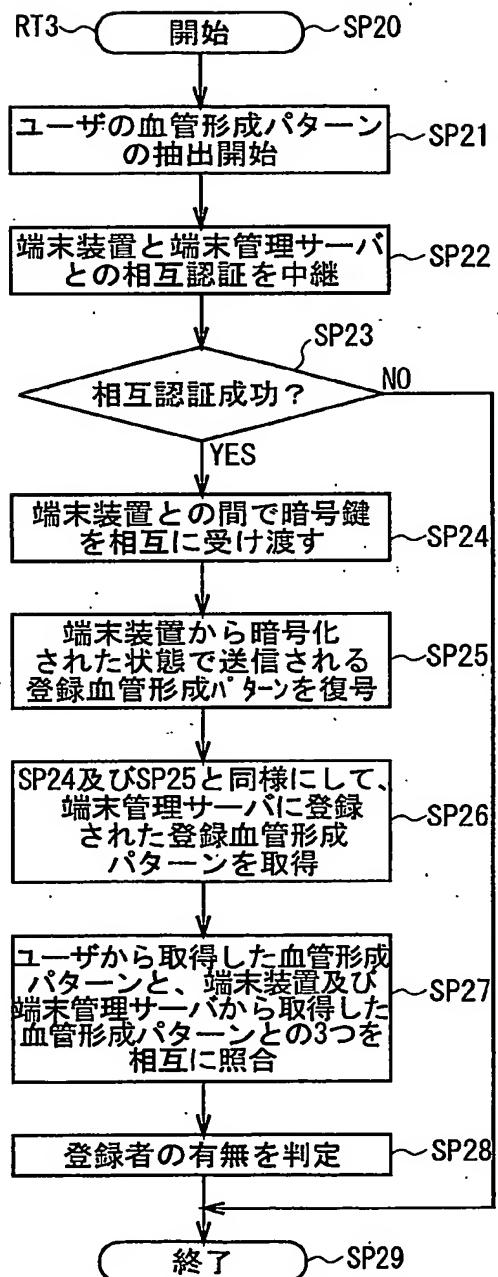


図 15

103 認証装置  
101

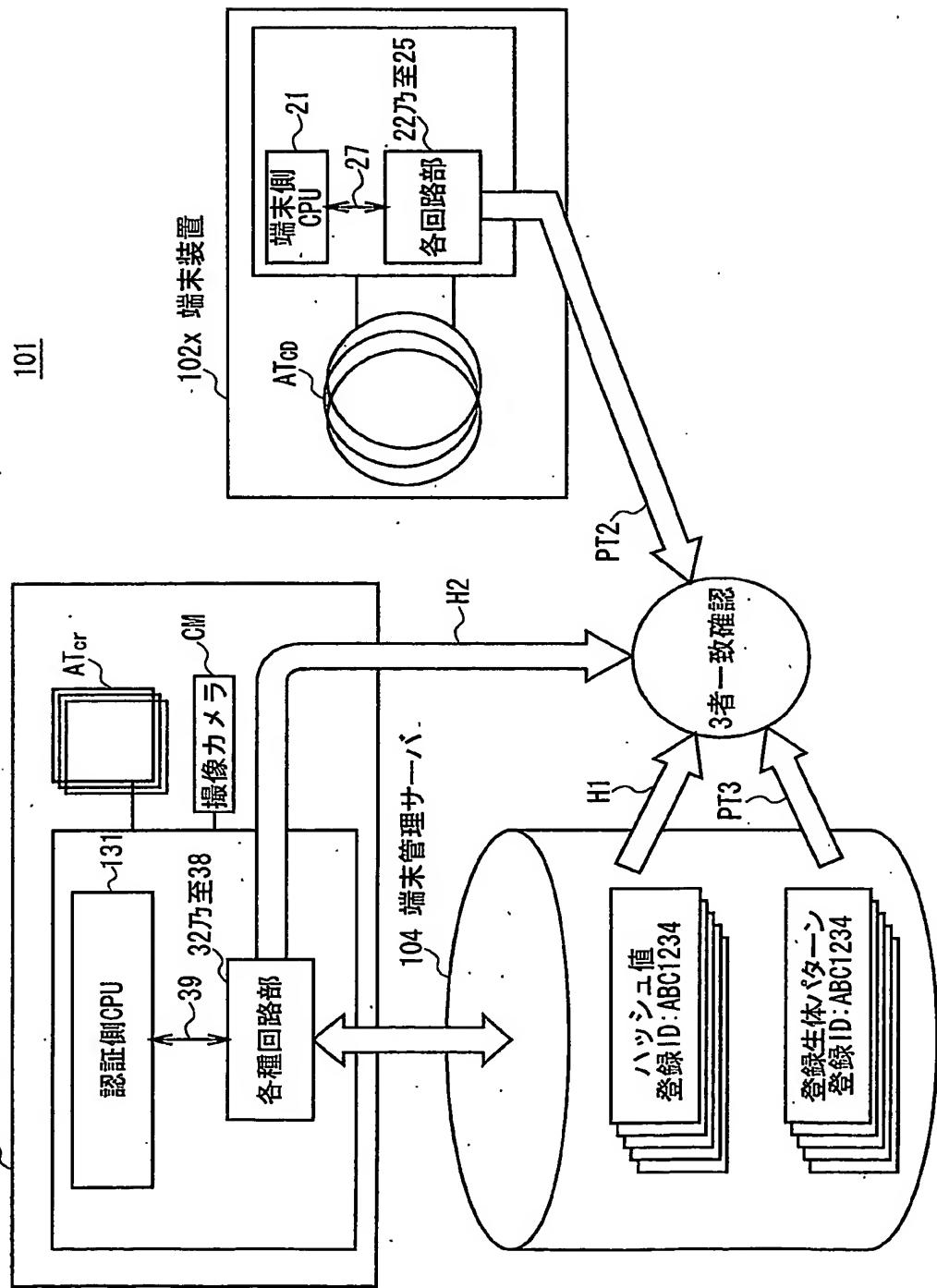


図16

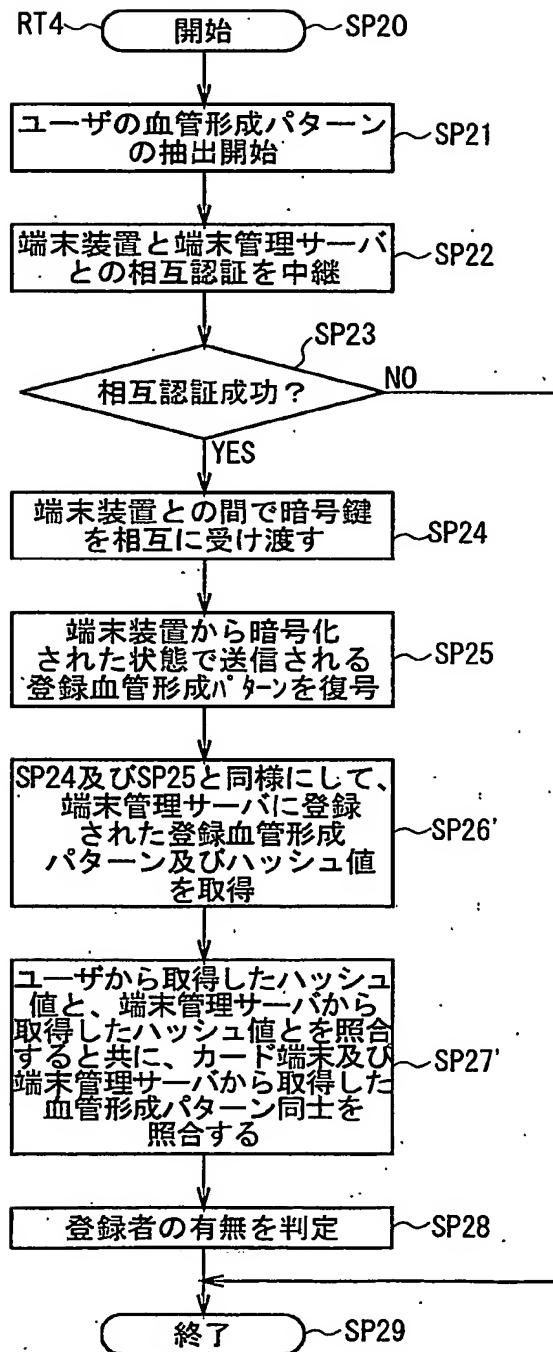


図 17

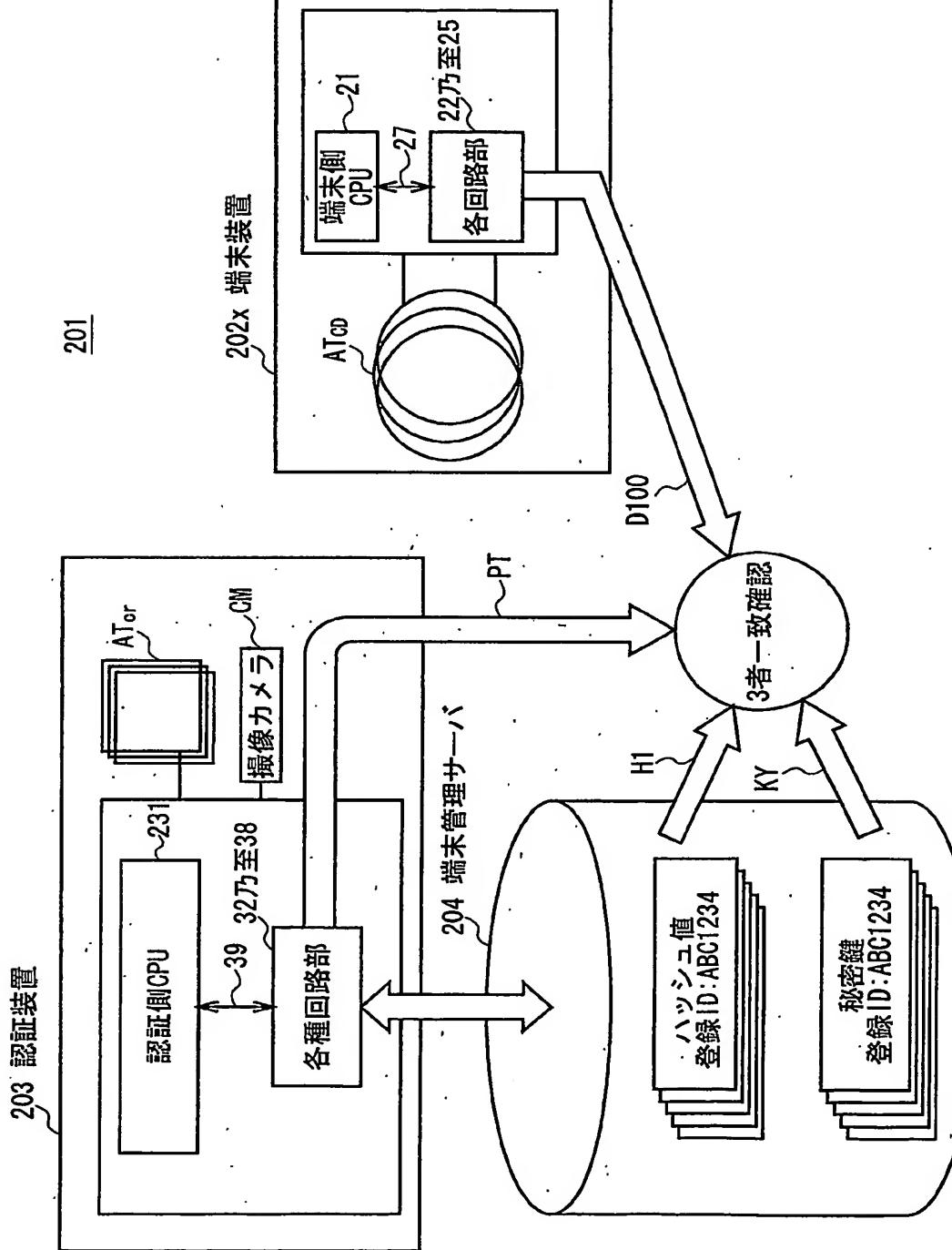


図 18

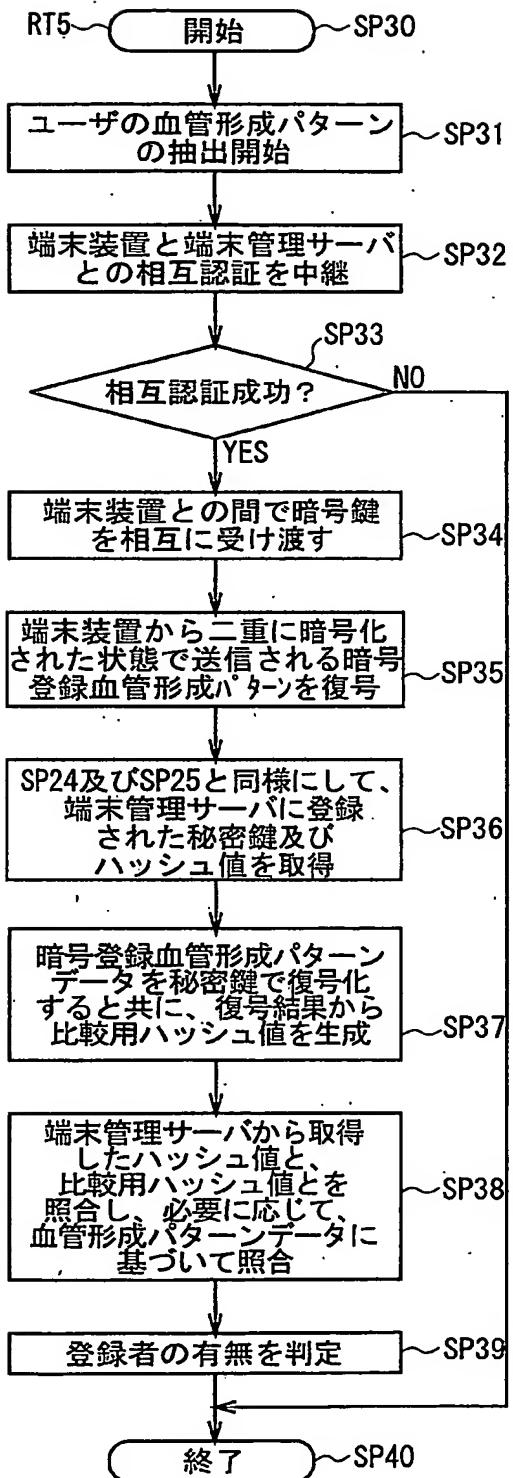
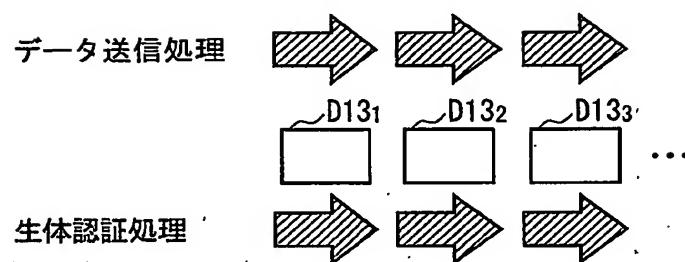


図 19

## (A) 通信エラーなしの場合



## (B) 通信エラーD132の場合

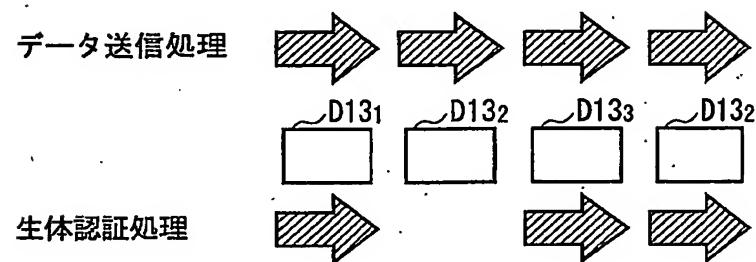


図 2 O

### 符 号 の 説 明

1、51、101、201……情報処理システム、2i (i=1、2、……、N)、  
2x……カード端末、52i (i=1、2、……、N)、52x……リング端末、10  
2x、202x……端末装置、3、53、103、203……認証装置、4……カード  
端末管理サーバ、104、204……端末管理サーバ、21、61……端末側CPU、  
31、71、131、231……認証側CPU、22、32……内部メモリ、23、3  
3……送受信部、24、34……暗号化／復号化部、25……乱数発生部、35……ネ  
ットワークインターフェース、36……駆動制御部、37、75……パターン抽出部、3  
8、77……認証部、73……ハードディスク、74……輝度パターン生成部、76  
……点滅パターン照合部、CM……撮像カメラ、LS……近赤外光光源、ATCD……  
端末側アンテナ、ATcr……認証側アンテナ、ICCD1、ICCD2……端末側信  
号処理部、ICcr1、ICcr2……認証側信号処理部、RT1……第1の認証処理  
手順、RT2……第2の認証処理手順、RT3……第3の認証処理手順、RT4……第  
4の認証処理手順、RT5……第5の認証処理手順